2015-16 ANNUAL REPORT

Office of the Information and Privacy Commissioner of Alberta

Office of the Information and Privacy Commissioner of Alberta

Office of the Information and Privacy Commissioner of Alberta
410, 9925 - 109 Street, NW
Edmonton, AB T5K 2J8

Phone: 780.422.6860
Toll Free: 1.888.878.4044
Fax: 780.422.5682
Email: generalinfo@oipc.ab.ca

www.oipc.ab.ca

NOVEMBER 2016

Office of the Information and
Privacy Commissioner of Alberta

November 2016

The Honourable Robert E. Wanner
Speaker
Legislative Assembly of Alberta
325 Legislature Building
10800 - 97 Avenue
Edmonton, AB
T5K 2B6

Dear Mr. Speaker:

I am honoured to present to the Legislative Assembly the Annual Report of the Office of the Information and Privacy Commissioner for the period April 1, 2015 to March 31, 2016.

This report is provided in accordance with section 63(1) of the *Freedom of Information and Protection of Privacy Act*, section 95(1) of the *Health Information Act*, and section 44(1) of the *Personal Information Protection Act*.

Original signed by
Jill Clayton
Information and Privacy Commissioner

Table of Contents

Commissioner's Message 6

About the Office 9
Mandate 10
OIPC Organizational Structure 2015-16 12
The Process: Request for Review/Complaint 13
OIPC as a Public Body 14
- FOIP Requests to OIPC 14
- OIPC Privacy Matters 14
- Proactive Travel and Expenses Disclosure 14
- Public Interest Disclosure Act 14

Financial Overview 15

Trends and Issues 17
Records Management and the Duty to Document 18
Breaches and Offences 19
PIPA Review and Global Considerations 20
Delays for Responding to Access Requests 21

By the Numbers 23
Graph A: Total Cases Opened 25
Graph B: Total Cases Closed 25
Table 1: Cases Opened by Case Type 26
Table 2: Cases Closed by Case Type 27
Table 3: Percentages of Cases Closed by Resolution Method 28
Graph C: Percentages of Cases Closed by Resolution Method 29
Table 4: General Enquiries 29

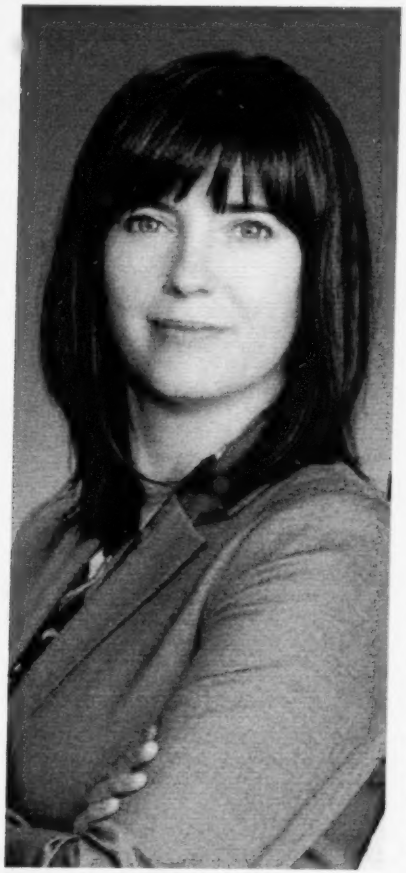
Regulation and Enforcement 31
Requests for Time Extensions under FOIP 32
Preliminary Review and Early Resolution Processes 32
Privacy Impact Assessment Reviews 33
Investigation Reports 34
Offence Investigations 37
Privacy Breach Reporting under HIA 37
Privacy Breach Reporting under FOIP 38
Privacy Breach Reporting under PIPA 38
Summary of Significant Decisions 41
Judicial Reviews and Other Court Decisions 44

Education and Outreach 47
OIPC Website Revamp 48
Presentations, Forums and Workshops 48
Collaboration with Other Jurisdictions 51
Media Awareness 52
Robert C. Clark Award 53

Financial Statements 55

Appendices 67
Appendix A: Cases Opened Under FOIP, HIA, PIPA by Entity 68
Appendix B: Cases Closed Under FOIP, HIA, PIPA by Entity 71
Appendix C: Orders and Public Investigation Reports Issued 74

Commissioner's Message



In considering the message I wanted to include in this year's Annual Report, I reflected on the events of the past year and also reviewed previous Annual Reports. I try to get a sense of what issues truly characterize a particular year and make it stand out, and also what distinguishes one year from another. This time around, undertaking this exercise solidified one thought for me in particular: access to information in Alberta is fast approaching a crisis situation.

This is not an entirely new phenomenon that just appeared out of nowhere. In my 2012-13 Annual Report I talked about Alberta's flawed access to information legislation – that Alberta tied for last in a report by the Centre for Law and Democracy that compared access to information legislation in various Canadian jurisdictions. I reported that my office had seen a 40% increase in cases opened under the *Freedom of Information and Protection of Privacy Act* (FOIP Act), and also an 89% increase in requests for time extensions (public bodies can apply to me for an extension of the time to respond to a request, provided they meet certain criteria under the Act).

I commented that recommendations following an all-party review of the FOIP Act in 2010 had not been implemented, but optimistically noted that the newly appointed Associate Minister responsible for Accountability, Transparency and Transformation had committed to a review of the Act. The public consultation for this review was completed in 2013 and the public was told that "the feedback from the consultation will be compiled into a summary report and posted online for further comment." To my knowledge, this information has never been made public.

The situation appeared to improve slightly in 2013-14 with the proactive disclosure of government travel and hospitality expenses, the launch of the government's Open Data Portal, and the first disclosures of salary and severance information for senior government employees.

My office's statistics, however, continued to show an increase in the number of new FOIP Act cases as well as the number of time extension requests; in addition, requests to excuse fees had skyrocketed (these are requests made to my office by applicants who would like a review of a public body's refusal to waive fees to respond to an access to information request).

The increase in the number of time extension requests is particularly notable, and was one of the factors that led to my announcement, in May 2014, of an investigation to look at how the government handles access to information requests under FOIP. The news release issued by my office read, in part, as follows:

- For some time, I have been concerned about the timeliness of responses to access requests. In my 2012-2013 Annual Report, I reported the number of requests for time extensions submitted to my Office increased by 89% from the previous fiscal year. The recent allegations raise questions about the reasons for the time extension requests.
- [Service Alberta] Statistics on the operations of the FOIP Act for the 2011-2012, 2012-2013 and 2013-2014 fiscal years are not available. While I have heard anecdotally that

government departments have seen increasing numbers of access requests, I have no statistics on these numbers or on the response times over the past three fiscal years.

- A number of applicants have informed my Office that public bodies do not respond to access requests within the timelines set out in the FOIP Act.
- Alberta's NDP Opposition and the Canadian Taxpayers Federation have publicly stated they have written to me asking for an investigation into delays in the release of records and raising concerns about political interference in the processing of access requests. I have received their written requests.
- I have heard anecdotally of concerns and allegations regarding the disclosure of applicant identities during the processing of access requests. This raises questions as to whether the identity of an applicant (e.g. political, media) is a factor in the time taken to respond to a request.[1]

Ironically, by the time I released my Annual Report for that year (2014-15), the investigation into possible delay was stalled in the courts. I reported:

> As part of the investigation, the OIPC requested documents from several Government of Alberta ministries. However, the information provided was redacted, sometimes quite heavily redacted, with no substantiation other than an assertion of "privilege". The Commissioner issued Notices to Produce records to 13 Government ministries, including Executive Council (the Premier's Office) and Alberta Justice and Solicitor General. The Government responded by bringing a judicial review application for all 13 ministries. The matter has been set down to be heard by the court in February 2016, some 21 months from the initiation of the investigation.[2]

The matter was not heard by the court in February 2016. Shortly after the government brought its judicial review application, Alberta's Court of Appeal issued its decision in *University of Calgary v. JR*, overturning a 2013 decision of the Court of Queen's Bench and finding that I do not have the power to compel production of records subject to solicitor-client privilege. I was granted leave to appeal this decision to the Supreme Court of Canada and the case was heard on April 1, 2016. As of writing, no decision has been issued.

Which brings me to 2015-16.

The number of time extension requests has increased again, this time by 60% (from 63 in 2014-15, to 101 in 2015-16). Of the 101 time extension requests received, 82% were made by government ministries.

There has been a significant increase in the number of deemed refusal files in my office, often by sophisticated public bodies that know their duties and obligations under the law (a deemed refusal is when an applicant has made an access request and has, essentially, not received any response). This has resulted in a number of orders requiring that public bodies respond to a request for access. I do not believe I should have to order public bodies to comply with a clear obligation under the law.

Finally, I do not know how widespread the problem of delay may be, nor possible reasons for delay such as whether there has been a significant increase in the volume of access requests received by public bodies. Service Alberta statistics on the operations of the FOIP Act are not available past 2012-2013 (as of time of writing).

My own 2014 investigation to review how the government handles access requests resulted in the government providing only heavily redacted documents to me and, as noted above, remains stalled in the courts.

What I do know is that Albertans are not receiving timely responses (or any response, in some cases) to their requests for access to information. I am calling on this government, and public bodies in all sectors, to reverse the course we are on and to demonstrate to Albertans respect for the values of transparency, accountability, and the law.

Jill Clayton
Information and Privacy Commissioner

[1] Office of the Information and Privacy Commissioner. "Commissioner Launches Investigation Into Government's Handling of Access Requests". May 30, 2014.
[2] Office of the Information and Privacy Commissioner. 2014-15 Annual Report, p. 20.

About the Office

Mandate

The Information and Privacy Commissioner is an Officer of the Legislature. The Commissioner reports directly to the Legislative Assembly of Alberta and is independent of the government.

Through the Office of the Information and Privacy Commissioner (OIPC), the Commissioner performs the legislative and regulatory responsibilities set out in Alberta's three access and privacy laws.

Freedom of Information and Protection of Privacy Act

The *Freedom of Information and Protection of Privacy Act* (FOIP Act) applies to 1,151 public bodies, including provincial government departments and agencies, boards and commissions, municipalities, Métis settlements, drainage districts, irrigation districts, housing management bodies, school boards, post-secondary institutions, public libraries, police services, police commissions and health authorities.

The FOIP Act provides a right of access to any record in the custody or under the control of a public body, subject to limited and specific exceptions. The Act also gives individuals the right to access their own personal information held by public bodies and to request corrections to their own personal information. The Act protects privacy by setting out the circumstances in which a public body may collect, use or disclose personal information.

Health Information Act

The *Health Information Act* (HIA) applies to more than 54,900 health custodians, including Alberta Health, Alberta Health Services, Covenant Health, nursing homes, physicians, registered nurses, pharmacists, optometrists, opticians, chiropractors, podiatrists, midwives, dentists, denturists and dental hygienists.

HIA also applies to "affiliates" who perform a service for custodians, such as employees, contractors, students and volunteers. Custodians are responsible for the information collected, used and disclosed by their affiliates.

HIA allows health services providers to exchange health information to provide care and to manage the health system.

The Act protects patients' privacy by regulating how health information may be collected, used and disclosed, and by establishing the duty for custodians to take reasonable steps to protect the confidentiality and security of health information. The Act also gives individuals the right to access their own health information, to request corrections, and to have custodians consider their wishes regarding how much of their health information is disclosed or made accessible through Alberta's provincial electronic health record system (i.e. Alberta Netcare).

Personal Information Protection Act

The *Personal Information Protection Act* (PIPA) applies to provincially-regulated private sector organizations, including businesses, corporations, associations, trade unions, private schools, private colleges, partnerships, professional regulatory organizations and any individual acting in a commercial capacity.

PIPA protects the privacy of clients, customers, employees and volunteers by establishing the rules for the collection, use and disclosure of personal information by organizations.

The Act seeks to balance the right of the individual to have his or her personal information protected with the need of organizations to collect, use or disclose personal information for reasonable purposes. PIPA also gives individuals the right to access their own personal information held by organizations and to request corrections.

The Commissioner oversees and enforces the administration of the Acts to ensure their purposes are achieved.

The Commissioner's powers, duties and functions include:

- Providing independent review and resolution on requests for review of responses to access to information requests and complaints related to the collection, use and disclosure of personal and health information
- Investigating any matters relating to the application of the Acts, whether or not a review is requested
- Conducting inquiries to decide questions of fact and law and issuing binding orders
- Educating the public about the Acts, their rights under the Acts and access and privacy issues in general
- Receiving comments from the public concerning the administration of the Acts
- Giving advice and recommendations of general application respecting the rights or obligations of stakeholders under the Acts
- Engaging in or commissioning research into any matter affecting the achievement of the purposes of the Acts
- Commenting on the implications for access to information or for protection of personal privacy of proposed legislative schemes and existing or proposed programs
- Commenting on the access and privacy implications of privacy impact assessments submitted to the Commissioner
- Commenting on the privacy and security implications of using or disclosing personal and health information for record linkages or for the purpose of performing data matching

Vision

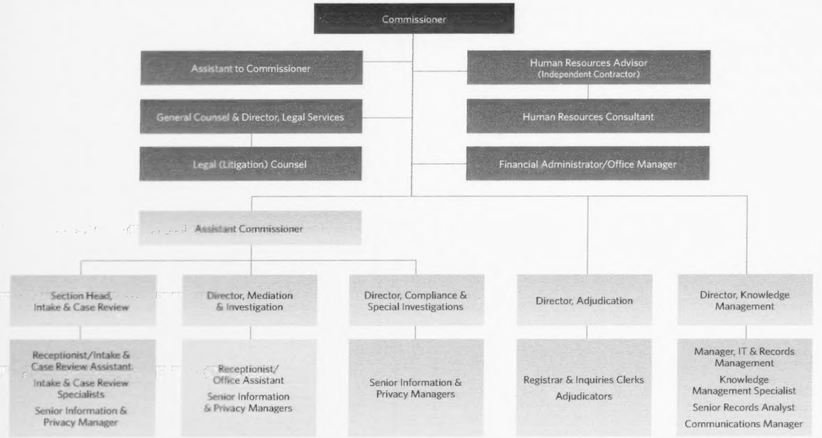
A society that values and respects access to information and personal privacy.

Mission

Our work toward supporting our vision includes:

- Advocating for the privacy and access rights of Albertans
- Ensuring public bodies, health custodians and private sector organizations uphold the access and privacy rights contained in the laws of Alberta
- Providing fair, independent and impartial reviews in a timely and efficient manner

OIPC Organizational Structure 2015-16



The Process: Request for Review/Complaint

Commissioner receives a request for review or complaint
Commissioner opens case and authorizes an officer to mediate/investigate[1]
Officer provides parties with findings and recommendations
Parties accept officer's findings and recommendations
Officer's findings and recommendations not accepted by one of the parties
Case resolved and closed
Applicant/Complainant asks to proceed to inquiry
Commissioner exercises discretion under FOIP/HIA/PIPA to refuse to conduct an inquiry
Commissioner/Adjudicator conducts inquiry
Commissioner/Adjudicator issues order

[1] **Note:** For more information, see Preliminary Review and Early Resolution Process in the Regulation and Enforcement section of this Annual Report (p. 32).

OIPC as a Public Body

FOIP Requests to OIPC

In 2015-16, the OIPC received five general information requests under the FOIP Act, and two informal requests for information. The OIPC responded to all of the requests within 30 days.

Section 4(1)(d) of the FOIP Act excludes from its operation a record that is created by or for or is in the custody or under the control of an officer of the Legislature and relates to the exercise of that officer's functions under an Act of Alberta.

From the 2014-15 fiscal year there were two outstanding matters related to information requests made to the OIPC.

To resolve one matter, an external adjudicator was designated by Order-in-Council to determine whether the OIPC properly excluded records subject to an access request after the applicant requested a review of the OIPC's decision. The request had initially been made to the OIPC in April 2014. The external adjudicator determined in September 2015 that the OIPC had properly excluded records because the requested records related to the exercise of the Commissioner's functions under the FOIP Act.

The second outstanding matter from 2014-15 was still unresolved at the end of 2015-16 awaiting a decision by an external adjudicator.

OIPC Privacy Matters

In 2015-16, the OIPC conducted one investigation into an internal incident.

The incident involved improper disposal of personal information from one of the OIPC's secure shredding boxes. A bag of documents that was meant to be shredded was improperly disposed of in the building's recycling bin, and then transported to a City of Edmonton recycling facility.

Drafts of letters to individuals who were corresponding with the OIPC were contained in the bag of documents, which included names and addresses of 12 affected individuals. After contacting the City of Edmonton and learning that it collects 2,000 tons of recycling material every day before being sent to China for processing, it was deemed unlikely that any of the material would be intercepted. Although there was no real risk of harm identified, the Commissioner notified all affected individuals.

Proactive Travel and Expenses Disclosure

The OIPC continues to publicly disclose the vehicle, travel and hosting expenses of the Commissioner, and the travel and hosting expenses of the Assistant Commissioner and OIPC Directors on a bi-monthly basis.

Public Interest Disclosure Act

No disclosures under the *Public Interest Disclosure Act* were received by the OIPC's designated officer in 2015-16.

Financial Overview

For the 2015-16 fiscal year, the total approved budget for the OIPC was $6,843,340. The total cost of operating expenses and capital purchases was $6.8 million. The OIPC returned $4,894 (0.1% of the total approved budget) to the Legislative Assembly.

Total Actual Costs Compared to Budget

	VOTED BUDGET	ACTUAL	DIFFERENCE
Operating Expenses*	$ 6,843,340	$ 6,838,446	$ 4,894
Capital Purchases	0	0	0
Total	**$ 6,843,340**	**$ 6,838,446**	**$ 4,894**

*Amortization is not included.

Salaries, wages, and employee benefits made up approximately 80% of the OIPC's operating expenses budget. Due to vacant positions and staff taking fewer courses, payroll related costs were $174,956 below budget. Legal fees were approximately $165,000 over budget due to the Commissioner's appeal to the Supreme Court of Canada. Appeal costs would typically be expensed over two fiscal years because of the length of time between the Court's granting leave to appeal and hearing the appeal. In this case, the Court granted the Commissioner leave to appeal and heard the appeal within a six-month period, resulting in appeal costs having to be expensed in one fiscal year. Technology services were $41,805 over budget due to changing to a more secure web hosting provider and developing a new website including a portal to prepare for the June 30, 2016 compensation disclosure requirements under the *Public Sector Compensation Transparency Act*. Various other supplies and services were under budget a net of approximately $37,000.

Total Actual Costs Compared to Prior Year

	2015-16	2014-15	DIFFERENCE
Operating Expenses	$ 6,838,446	$ 6,770,462	$ 67,984
Capital Purchases	0	18,651	(18,651)
Total	**$ 6,838,446**	**$ 6,789,113**	**$ 49,333**

Total costs for operating expenses and equipment purchases increased by $49,333 from the prior year. The increase was primarily due to an increase in base salaries from a mandated cost of living allowance and merit increases to staff, where applicable. The increase to Salaries, Wages and Benefits of $281,816 was offset by a reduction in costs for Supplies and Services of $213,832. There was also a reduction of $18,651 as there were no capital expenditures in the current year. In addition, operating expenses were controlled by not hiring staff to fill two vacant full time positions.

Trends & Issues

This section provides context for some of the work of the OIPC by highlighting provincial, national and international issues and trends that shape and influence the access and privacy landscape.

Records Management and the Duty to Document

Records management was in the public spotlight on numerous occasions throughout 2015-16 in Alberta and abroad.

At home, in the wake of the 2015 provincial election, the discussion centred on the destruction of records. Concerns expressed on social media were relayed by the media and the Commissioner received letters about records destruction at Alberta Environment and Sustainable Resource Development, and generally within the Government of Alberta.

At the same time, the Public Interest Commissioner received a disclosure of wrongdoing under the *Public Interest Disclosure (Whistleblower Protection) Act* related to the possible destruction of records in a ministerial correspondence tracking application, the Action Request Tracking System. The Commissioner and Public Interest Commissioner opened a joint investigation into the allegations of improper destruction of records by Alberta Environment and Sustainable Resource Development a week following the provincial election. (The results of the investigation were released in January 2016 and summarized in the Regulation and Enforcement section of this Annual Report.)

Beyond Alberta's borders, a report condemning the records management practices of the British Columbia government was released by the Office of the Information and Privacy Commissioner for British Columbia. The investigation highlighted, in part, what was colloquially known as the "triple delete scandal" where it was found that records subject to access requests were being wilfully deleted by government officials. In three separate cases, the investigation found contraventions of access and privacy law. In relation to the "triple delete scandal" one former staffer was eventually charged with two counts of wilfully making false statements to mislead, or attempt to mislead.

In Ontario, after Ontario's Information and Privacy Commissioner ruled that government officials broke access and privacy law by deleting all emails related to the cancellation of gas plants in 2013, top officials were charged in December 2015 with breach of trust, mischief in relation to data and misuse of a computer system to commit the offence of mischief. The trials for those charged are to be heard in 2017.

South of the Canadian border, much attention was paid to Presidential-hopeful Hillary Clinton's use of private email servers to conduct government business while she held the position of Secretary of State.

In response to these and other developments, the Information Commissioners of Canada issued a joint statement in February 2016 calling on governments at all levels to create a legislated duty to document. A duty to document would require public entities to document matters related to their deliberations, actions and decisions. Information Commissioners had noted a trend of no records responses to access to information requests.

This joint statement echoed the Alberta Commissioner's recommendations to the Government of Alberta's 2013 review of the FOIP Act. The Commissioner's submission stated that government should consider amending the FOIP Act to require public bodies to "create such records as are reasonably necessary to document their decisions, actions, advice, recommendations and deliberations" and "ensure that all records are covered in records retention and disposition schedules."

Breaches and Offences

Privacy breaches continued to be an issue in 2015-16. The OIPC received 311 self-reported breaches representing a 22% increase over 2014-15 (255). Accounting for the most significant increase was under HIA where there were 70% more self-reported breaches – from 76 in 2014-15 to 129 in 2015-16.

The types of breaches being reported to the office vary – from human error to highly sophisticated cyberattacks. These incidents can affect a single individual to thousands of individuals. Any public body, custodian or organization is susceptible to a breach of personal or health information.

As technology advances so too do cyberattacks. But there continue to be breaches of personal or health information that are preventable. For instance, more than a decade has passed since the office first called on public bodies, custodians and organizations to encrypt mobile devices, yet a significant proportion of reported incidents involve the theft or loss of unencrypted devices containing personal or health information. Meantime, the issue of employee "snooping" continues, most notably in the health sector where in 2015-16 alone four individuals faced charges for unauthorized access to health information under HIA.

In response to cyberattacks, the OIPC issued an *Advisory for Ransomware* in an attempt to get out in front of a type of malware that is wreaking havoc at a variety of institutions around the world. And in preparation for upcoming breach provisions under HIA, the office released its investigation into the health sector's preparedness for breach reporting in December 2015. The office also began to offer a breach response and reporting workshop, which was introduced at the OIPC's 2016 Data Privacy Day event in Calgary on January 28.

Legislative Reform

Many developments also occurred legislatively with regard to mandatory breach reporting and notification.

Alberta is a leader for mandatory breach reporting and notification in the private sector. The province became the first jurisdiction in Canada to have these mandatory breach provisions in 2010. In 2014, the Alberta government also passed amendments to HIA for mandatory breach reporting and notification provisions, as well as new offence provisions for failing to report a breach, but these have not come into force.

Over the past few years, other jurisdictions have started following in Alberta's footsteps:

- Under the federal private sector privacy legislation, the *Personal Information Protection and Electronic Documents Act*, mandatory breach provisions were passed in April 2014 but continue to await supporting regulations to be in force.
- In Ontario, the *Personal Health Information Protection Act* had changes slated to be in force in June 2016 that included mandatory breach reporting and notification, as well as new offence provisions for failing to report a breach.
- Manitoba's *Personal Information Protection and Identity Theft Prevention Act* included mandatory notification requirements to individuals (but not to the Ombudsman). It was passed in 2013 but is awaiting proclamation.
- Newfoundland and Labrador became the first jurisdiction in Canada to include mandatory breach provisions under its public sector access and privacy law, the *Access to Information and Protection of Privacy Act*, 2015. These historic amendments came into force on June 1, 2015.

Meantime, in several jurisdictions movement was afoot to include mandatory breach provisions, such as Saskatchewan's *Health Information Protection Act*, and British Columbia's *Personal Information Protection Act* where the committee tasked with reviewing the legislation recommended such provisions in February 2015.

PIPA Review and Global Considerations

In June 2015, the Standing Committee on Alberta's Economic Future was tasked with a review of PIPA. Within 18 months, the committee must submit its report and recommended amendments to the Legislative Assembly.

As part of its review, the committee solicited feedback from stakeholders. The Commissioner submitted 10 recommendations in February 2016 that considered global developments in private sector privacy law, namely discussions on the European Union's *General Data Protection Regulation* (GDPR) and the striking down of Safe Harbor, the EU-United States pact for personal information processing activities.

PIPA is a made-in-Alberta approach to balancing the privacy interests of Albertans and the legitimate collection, use and disclosure of personal information by organizations for reasonable purposes. But PIPA was not created in a vacuum. There are other global forces and principles that shaped how PIPA was drafted and how it must function in order to be recognized within Canada and by other nations.

Specifically, in 2015-16, the EU was nearing the finalization of the GDPR that was anticipated to shift the privacy policy and governance landscape. The GDPR, once passed, would supersede the *Data Protection Directive*, which was passed in 1995 and required each member state to implement its own privacy law.

The significant changes contained within GDPR will make privacy law across Europe stricter and enhance the protections for Europeans' personal information. In effect, GDPR will have reverberations for businesses around the world.

It is noteworthy, however, that Alberta is already ahead of the curve with mandated breach reporting and notification requirements, which were enacted in 2010 – in fact, Alberta is the only private sector jurisdiction in Canada that has these provisions and Canada and British Columbia are working to catch up. The GDPR will include similar breach provisions.

In addition, the office's work with the Office of the Privacy Commissioner of Canada and Office of the Information and Privacy Commissioner for British Columbia to publish *Getting Accountability Right with a Privacy Management Program* in 2012 anticipated and is aligned with the new legal requirements in the GDPR around privacy management frameworks.

In a global economy where private sector privacy law needs to be aligned with global and national legislation, and where private sector businesses are looking for certainty and consistency to the extent possible in the many jurisdictions in which they operate, the Commissioner made recommendations that were mindful of amendments that might weaken the legislation, or that would be out of step with global and national considerations.

Delays for Responding to Access Requests

Two related issues raised questions about the ability of public bodies, and specifically government ministries, to respond to access requests in the time limits set out in the FOIP Act. In 2015-16, the OIPC had a substantial increase in the number of requests for time extensions and implemented a new process for handling matters where the public body acknowledged it had not responded to applicants in time (deemed refusals).

Requests for Time Extensions

One persisting trend which amplified in 2015-16 was the increased number of time extension requests public bodies submitted to the OIPC. There was a 60% increase in the number of time extension requests received in 2015-16 (101) over 2014-15 (63).

This increase raises questions about the number, size and complexity of access requests received by public bodies, and their ability to respond to them. A public body must make every reasonable effort to respond to a request for access under the FOIP Act within 30 calendar days. A public body may ask the OIPC for a time extension in specific and limited situations set out in the FOIP Act (section 14).

In 2015-16, as part of its focus on continuous process improvement, the OIPC reviewed its management of requests for time extensions. The OIPC sought feedback from public bodies and began revising its form and developing a practice note to assist public bodies in their preparation and submission of time extension requests. Essentially, the OIPC intended to identify the fundamental factors required to make an informed decision to grant or deny a request for time extension and to communicate these factors to public bodies.

Despite steps taken to improve processes to manage time extension requests, it is not enough. Significant issues with requests for time extensions remain because of the FOIP Act itself, and amendments continue to be recommended by the Commissioner.

Of the 101 time extension requests received:

- 82% were made by provincial government ministries
- 8% were made by municipalities
- 5% were made by law enforcement
- 4% were made by school districts
- 1% was made by a university

The Commissioner's submission to the 2013 FOIP Act review made a number of recommendations pertaining to time extensions (sections 14, 30 and 31). For example, in unforeseen disaster situations, the FOIP Act does not allow a public body to grant itself a time extension if it cannot access records nor does it allow the Commissioner to grant a time extension based on such emergency circumstances.

Other recommendations related to clarifying time extension portions of the FOIP Act to improve the process for applicants, public bodies and the OIPC, and to limit the number of interpretations that arise from sections related to time extensions.

In addition, the rapidly increasing number of time extension submissions raises a question as to whether public bodies have the resources necessary to meet their duty to make every reasonable effort to respond to access requests in 30 days.

Deemed Refusals to Respond

Related to the concerns raised with requests for time extensions, there were five Orders issued by the OIPC where the only issue at inquiry was the time limit for responding to the applicants' access requests.

In each of the Orders, the public bodies – all government ministries – acknowledged their failure to respond to the applicants in the mandated time limits. As part of the reason for not responding, the public bodies indicated staff shortages. Further, complexity of the request was noted in one case. However, under the FOIP Act, these are not sufficient reasons to not respond to applicants and the public bodies were found not to be upholding the access rights of applicants.

In each of the five Orders, the Adjudicators recognized the limitations of the public bodies to respond within the legislated timeframe but ordered them to respond to applicants' access requests because the time limits for responding are mandatory under the FOIP Act.

By the Numbers

Self-Reported Breaches Closed:

65% ↑

84% ↑ under FOIP

58% ↑ under HIA

65% ↑ under PIPA

Privacy Impact Assessments Submitted:

27% ↑

25% ↑ under HIA

82% of total under HIA were from physicians, pharmacists and chiropractors

HIA Complaints:

85% ↑

Requests for Time Extensions under FOIP:

60% ↑

Number of Presentations:

74

Media Requests:

105

Total Cases Opened

(excluding Intake cases):

13% ↑

36% ↑ under HIA

Total Cases Closed

(excluding Intake cases):

19% ↑

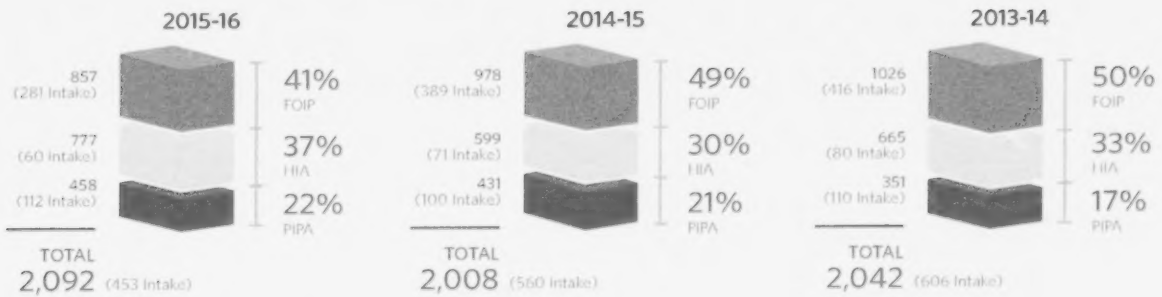
Self-Reported Breaches Opened:

22% ↑

70% ↑ under HIA

Graph A: Total Cases Opened

Three Year Comparison



Graph B: Total Cases Closed

Three Year Comparison

Table 1: Cases Opened by Case Type

FOIP	2015-16	2014-15	2013-14
Advice and Direction	0	0	1
Authorization to Disregard a Request	3	7	0
Complaint	78	85	91
Disclosure to Commissioner (Whistleblower)	0	1	1
Engage in or Commission a Study	0	0	2
Excuse Fees	10	7	33
Investigation Generated by Commissioner	13	23	5
Notification to OIPC	7	8	4
Offence Investigation	0	2	0
Privacy Impact Assessment	22	12	14
Request Authorization to Indirectly Collect	0	0	1
Request for Information	14	24	26
Request for Review	255	294	303
Request for Review 3rd Party	35	22	26
Request Time Extension	101	63	81
Self-reported Breach	38	41	22
Sub-Total	**576**	**589**	**610**
Intake Cases	**281**	**389**	**416**
Overall Total	**857**	**978**	**1026**

HIA	2015-16	2014-15	2013-14
Advice and Direction	0	0	0
Authorization to Disregard a Request	1	1	0
Complaint	72	39	50
Engage in or Commission a Study	0	0	0
Excuse Fees	0	1	0
Investigation Generated by Commissioner	28	28	15
Notification to OIPC	0	0	0
Offence Investigation	1	2	4
Privacy Impact Assessment	427	341	369
Request for Information	33	24	33
Request for Review	26	16	46
Request Time Extension	0	0	0
Self-reported Breach	129	76	68
Sub-Total	**717**	**528**	**585**
Intake Cases	**60**	**71**	**80**
Overall Total	**777**	**599**	**665**

PIPA	2015-16	2014-15	2013-14
Advice and Direction	0	0	0
Authorization to Disregard a Request	2	0	0
Complaint	129	121	75
Engage in or Commission a Study	0	0	0
Excuse Fees	0	0	0
Investigation Generated by Commissioner	5	7	14
Notification to OIPC	0	0	0
Offence Investigation	1	0	0
Privacy Impact Assessment	3	3	1
Request for Advance Ruling	0	0	0
Request for Information	8	9	3
Request for Review	54	52	52
Request Time Extension	0	1	0
Self-reported Breach	144	138	96
Sub-Total	**346**	**331**	**241**
Intake Cases	**112**	**100**	**110**
Overall Total	**458**	**431**	**351**

Notes: (1) See Appendix A for a complete listing of cases opened in 2015-16.

(2) Only FOIP allows a 3rd Party to request a review of a decision to release 3rd party information to an applicant.

(3) Intake cases include determining whether parties coming to the OIPC are properly exercising the rights set out in FOIP, HIA and PIPA; whether the matters or issues identified by the parties are within the Commissioner's legislative jurisdiction; and investigating and trying to resolve certain requests or complaints.

Table 2: Cases Closed by Case Type

FOIP	2015-16	2014-15	2013-14
Advice and Direction	0	0	1
Authorization to Disregard a Request	4	4	1
Complaint	76	117	77
Disclosure to Commissioner (Whistleblower)	0	0	1
Engage in or Commission a Study	0	0	0
Excuse Fees	6	25	12
Investigation Generated by Commissioner	4	7	6
Notification to OIPC	7	8	4
Offence Investigation	0	0	0
Privacy Impact Assessment	18	16	13
Request Authorization to Indirectly Collect	0	0	1
Request for Information	12	29	22
Request for Review	292	230	258
Request for Review 3rd Party	31	24	26
Request Time Extension	93	64	90
Self-reported Breach	48	26	21
Sub-Total	**591**	**550**	**533**
Intake Cases	**281**	**405**	**392**
Overall Total	**872**	**955**	**925**

HIA	2015-16	2014-15	2013-14
Advice and Direction	0	0	0
Authorization to Disregard a Request	1	1	0
Complaint	39	42	15
Engage in or Commission a Study	0	0	0
Excuse Fees	1	0	0
Investigation Generated by Commissioner	16	18	13
Notification to OIPC	0	0	0
Offence Investigation	1	1	0
Privacy Impact Assessment	415	340	344
Request for Information	33	21	29
Request for Review	31	9	17
Request Time Extension	0	0	0
Self-reported Breach	112	71	40
Sub-Total	**649**	**503**	**458**
Intake Cases	**68**	**68**	**71**
Overall Total	**717**	**571**	**529**

PIPA	2015-16	2014-15	2013-14
Advice and Direction	0	0	0
Authorization to Disregard a Request	0	2	0
Complaint	111	114	50
Engage in or Commission a Study	0	0	0
Excuse Fees	0	0	0
Investigation Generated by Commissioner	6	12	4
Notification to OIPC	0	0	0
Offence Investigation	0	0	0
Privacy Impact Assessment	4	3	0
Request for Advance Ruling	0	0	0
Request for Information	8	6	7
Request for Review	70	44	41
Request Time Extension	0	1	0
Self-reported Breach	125	76	66
Sub-Total	**324**	**258**	**168**
Intake Cases	**122**	**100**	**84**
Overall Total	**446**	**358**	**252**

Notes: (1) See Appendix B for a complete listing of cases closed in 2015-16.

(2) A listing of all privacy impact assessments accepted in 2015-16 is available on the OIPC website at www.oipc.ab.ca.

(3) Only FOIP allows a 3rd Party to request a review of a decision to release 3rd party information to an applicant.

(4) Intake cases include determining whether parties coming to the OIPC are properly exercising the rights set out in FOIP, HIA and PIPA; whether the matters or issues identified by the parties are within the Commissioner's legislative jurisdiction; and investigating and trying to resolve certain requests or complaints.

Table 3: Percentage of Cases Closed by Resolution Method

Under the Acts only certain case types can proceed to Inquiry if the matters are not resolved at Mediation/Investigation. The statistics below are those case types that can proceed to Inquiry (Request for Review, Request for Review 3rd Party, Request to Excuse Fees, and Complaint files).

RESOLUTION METHOD	NUMBER OF CASES (FOIP)	NUMBER OF CASES (HIA)	NUMBER OF CASES (PIPA)	TOTAL	%
Resolved by Mediation/Investigation	337	51	157	545	83%
Resolved by Order or Decision	37	9	18	64	10%
Resolved by Commissioner's decision to refuse to conduct an Inquiry	17	10	4	31	5%
Withdrawn during Inquiry process	7	0	1	8	1%
Discontinued during Inquiry process	7	1	1	9	1%
Total	405	71	181	657	100%

FOIP Orders: 36 (37 cases); HIA Orders: 9 (9 cases); PIPA Orders: 13 (18 cases); no Decisions were issued under FOIP, HIA or PIPA in 2015-16

Notes: (1) This table includes only the Orders and Decisions issued that concluded/closed a file. See Appendix C for a list of all Orders, Decisions and Public Investigation Reports issued in 2015-16. Copies of all Orders, Decisions and Public Investigation Reports are available on the OIPC website www.oipc.ab.ca

(2) Orders and Decisions are recorded by the date the Order or Decision was signed, not the date the Order or Decision was publicly released.

(3) Three FOIP case files were closed by a single Order.

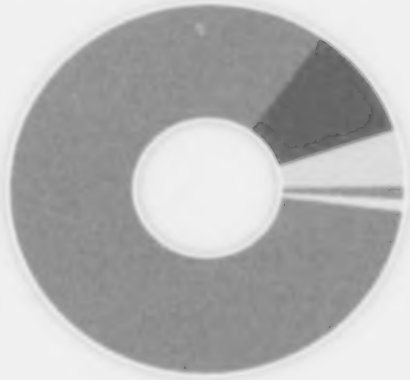
(4) Three PIPA case files were closed by a single Order.

(5) Six PIPA case files were closed by three Orders (i.e. two case files were closed per Order).

(6) Discontinued during the Inquiry process includes one FOIP case file that was discontinued before a decision was made to hold an Inquiry.

(7) An Inquiry can be discontinued due to a lack of contact with or participation by the applicant or complainant or because the issues have become moot.

Graph C: Percentage of Cases Closed by Resolution Method



- 83%
- 10%
- 5%
- 1%
- 1%

Of the 657 cases that could proceed to inquiry:

13% were resolved within 90 days

24% were resolved within 91 to 180 days

63% took more than 180 days to resolve

Table 4: General Enquiries

Telephone Calls		
FOIP	**Number**	**Percentage**
Public Bodies	176	32%
Individuals	376	68%
Total	**552**	**100%**
HIA	**Number**	**Percentage**
Custodians	301	48%
Individuals	322	52%
Total	**623**	**100%**
PIPA	**Number**	**Percentage**
Organizations	333	30%
Individuals	777	70%
Total	**1110**	**100%**
Emails	**405**	
Non-jurisdictional	**292**	
Total	**2,982**	

Regulation & Enforcement

Requests for Time Extensions under FOIP

In 2015-16, there was a 60% increase in the number of time extension requests received in 2015-16 (101) over 2014-15 (63). Of the 101 time extension requests received, 82% were made by provincial government ministries.

A public body must make every reasonable effort to respond to a request for access under the FOIP Act within 30 calendar days. A public body may ask the OIPC for a time extension in specific and limited situations set out in the FOIP Act (section 14).

Of the 101 requests received in 2015-16:

- 54 (53%) were granted as requested
- 21 (21%) were partially granted (extension period permitted was less than what was requested by the public body)
- 15 (15%) were denied
- 11 (11%) were withdrawn by the public body

Preliminary Review and Early Resolution Processes

To effectively manage case load pressures the OIPC has been experiencing, the office began utilizing new processes to resolve certain files as quickly as possible.

Essentially, files are being assessed in terms of complexity and the amount of work required once received to direct it to an appropriate resolution process. The files selected for early resolution tend to deal with a moderate to minimal number of records (e.g. 300 records or less) with few exceptions to disclosure applied by public bodies, custodians or organizations.

The following processes have resulted in additional records being released, further information being provided to applicants explaining the exceptions being applied, or complaints being resolved when the public body, custodian or organization are given an opportunity to respond directly to the applicant or complainant.

Requests for Review

In requests for review concerning responses to access requests, a preliminary assessment is conducted to determine complexity of the file and how the Acts were applied.

During the preliminary assessment, if it is determined that the file can be mediated by telephone or email the file remains with the preliminary assessor to resolve. If not, it will be assigned to another staff member.

One significant aspect of this process is that in the opening letter for cases the Commissioner asks public bodies, custodians and organizations to provide records to the OIPC quicker so the office can more efficiently determine whether a case may be resolved through the preliminary assessment process.

Complaints

For complaints regarding collection, use or disclosure of personal information, the OIPC identifies files for the "triage process" at the outset. These are files determined to be more amenable to early resolution.

For these complaints, similar to the request for review preliminary process, the outcome under the law may quickly be resolved by telephone or email. For example, where a complaint has been made regarding disclosure of personal information without consent under PIPA, but the authority for the disclosure is clearly authorized by another law.

Again, similar to request for review assessments, if complaint files are not resolved at the triage phase – due to the complexity or a requirement to gather more formal written submissions – the file is assigned to another staff member.

Proactive Party Resolution

The OIPC has also adopted a "proactive party resolution" approach to resolving files. If the office determines that the parties have not explored all options between themselves, the office will open a file but will first encourage the parties to resolve the matter prior to the office mediating the issue.

Privacy Impact Assessment Reviews

A privacy impact assessment (PIA) is a process of analysis that helps to identify and address potential privacy risks that may occur in the operation of a new or redesigned project. PIAs are recommended to be completed during the planning phase of a project.

A PIA is meant for proposed legislative schemes, administrative practices and/or information systems that relate to the collection, use or disclosure of individually identifying personal or health information. A PIA describes the initiative and its benefits, analyzes legal authority to collect, use or disclose personal or health information, assesses privacy risk and mitigation plans, and explains the policy management structure in place.

PIA Overview

In 2015-16, the OIPC accepted 437 PIAs. This represented a 22% increase over 2014-15 (359).

A vast majority (95% or 415) of PIAs were accepted under HIA because of mandatory PIA requirements (section 64). The OIPC accepted 18 PIAs from public bodies subject to the FOIP Act, while four PIAs were accepted from PIPA organizations.

A listing of all PIAs accepted in 2015-16 is available at www.oipc.ab.ca.

HIA

In total, there were 415 PIAs accepted by the OIPC under HIA.

Of the 415 accepted PIAs under HIA,

82%

were from physicians (187), pharmacies/pharmacists (95) and chiropractors (57).

Of note, the OIPC accepted a PIA from Alberta Health and Alberta Health Services on the Personal Health Portal. This collaborative project is meant to provide custodians with an integrated source of health information related to their patients, and is also intended to provide Albertans with an ability to have more control over their health information and provide tools to manage the health services available to them.

In addition, some physician offices had their PIAs accepted on physician and patient portals for electronic medical records. Among the features, these systems are intended to allow physicians to electronically access patient information through mobile apps, as well as providing patients access to their own health information electronically.

FOIP Act

The OIPC reviewed and accepted 18 PIAs from public bodies.

Notably, the Anti-Money Laundering Unit at the Alberta Gaming and Liquor Commission submitted a PIA on its anti-money laundering reporting program as required by the federal Financial Transactions and Reports Analysis Centre (FINTRAC). Previously, facilities (i.e. casinos) had been responsible and accountable for reporting anti-money laundering transactions to FINTRAC but, starting in July 2015, FINTRAC stipulated that AGLC would be accountable for reporting these transactions. The OIPC accepted the PIA on the in-house solution AGLC had developed for its reporting requirements to FINTRAC.

The OIPC also accepted a PIA submitted by Alberta Education on its Provincial Approach to Student Information. This system provides students with online access to their personal academic information.

As noted in last year's annual report, and continued in 2015-16, some of the PIAs reviewed and accepted by the OIPC related to cloud services for education.

Further, the City of Cold Lake submitted PIAs for its policy on surveillance cameras in public areas.

PIPA

In 2014-15, the OIPC accepted its first PIA for usage-based insurance (UBI) from an organization preparing to enter the Alberta market. There were two more PIAs for UBI accepted by the OIPC in 2015-16. There were two other PIAs from organizations that were accepted by the OIPC.

UBI programs provide auto insurance customers with the potential to receive discounts based on their driving habits. Some of the customers' driving habits are recorded on a telematics device installed in their vehicle and the information collected is transmitted wirelessly to the insurance provider. This type of insurance was to be made available to Albertans in April 2016.

The OIPC was pleased with the approach taken by Alberta's Superintendent of Insurance (Alberta Treasury Board and Finance) with regard to UBI. For an insurer looking to implement UBI in Alberta, the Superintendent of Insurance requires insurers to follow a process that included the submission of a PIA to the OIPC for review and acceptance. To help insurers meet that requirement, the OIPC published *Privacy Impact Assessment Guidelines for Insurers Looking to Implement Usage-Based Insurance Programs in Alberta.*

Under UBI programs, auto insurance customers can receive discounts based on their driving habits, which are recorded on a telematics device in the vehicle and transmitted to the insurance provider wirelessly.

Investigation Reports

Public Service Salary, Benefit and Severance Disclosure

In November 2015, the OIPC published its investigation report on the disclosure of public service salary, benefit and severance information. This disclosure of personal information was required under the government's *Public Service Compensation Disclosure Policy.* The investigation into the disclosure was opened on the Commissioner's own motion.

The investigation found that, in general, the collection, use and disclosure of personal information was not in compliance with the *Freedom of Information and Protection of Privacy Act* (FOIP Act) during the period of January 7 to 20, 2014, when activities were underway to prepare for the January 31, 2014 disclosure. On January 20, 2014, a Treasury Board directive was signed giving effect to the policy. Once signed, the directive – an "enactment" under the FOIP Act – authorized the collection, use and disclosure of personal information.

As the Commissioner noted in the report, "Some may see this as mere technical non-compliance with the FOIP Act during the period of January 7 to 20, 2014... In my view, however, this situation speaks to the need for all public bodies contemplating a new initiative with potential access and privacy implications to identify the risks and clearly identify their authority under the FOIP Act before moving forward."

The report was timely as just two weeks previous to its release, on November 5, 2015, the government announced it was moving forward with Bill 5, the *Public Sector Compensation Transparency Act.* That Act, once passed, requires all agencies, boards, commissions and legislative offices to disclose compensation, among other, information of employees whose compensation meets a threshold established in the legislation. The first disclosure was required by June 30, 2016 and will be required each subsequent year by that date.

Alleged Improper Destruction of Records by Alberta Environment and Sustainable Resource Development

In the wake of the 2015 provincial election, a number of traditional and social media reports surfaced about the widespread destruction of government records. The Commissioner also received letters expressing concern about the alleged improper destruction of records. Further, a disclosure of wrongdoing was made to the Public Interest Commissioner in relation to Alberta Environment and Sustainable Resource Development (ESRD).

The Commissioner and Public Interest Commissioner authorized a joint investigation, the first of its kind between the two Officers of the Legislature.

Of the four investigation objectives, three objectives concerned the OIPC and the FOIP Act.

Key findings from the investigation included:

- There was no direct monitoring or review of the management or destruction of records kept at the Minister's office.
- The destruction of 344 boxes of ESRD executive records was not in compliance with the rules related to the destruction of records.
- The security arrangements made by ESRD to protect against unauthorized destruction of records in the Action Request Tracking System (ARTS) were not reasonable.
- Records schedules were found to be confusing, overlapping and difficult to apply.
- There appeared to be a serious misunderstanding on the part of some Service Alberta officials as to the application of the FOIP Act to records in ARTS.
- Program support, monitoring and accountability for the records destruction process at ESRD was inadequate and presented an unreasonable level of risk that records may be destroyed in contravention of the *Records Management Regulation* (RM Regulation).
- There was no evidence that records were destroyed with the intent to evade an access request.
- With regard to the specific allegation made to the Public Interest Commissioner (i.e. the destruction of records in ARTS), the investigation found no evidence that records in ARTS were destroyed.

Among the 16 recommendations made:

- Identify gaps, and clarify policies, procedures and responsibilities to ensure records are identified, preserved and appropriately restricted at all times, especially during a period of government transition.
- Identify and address gaps in the monitoring of records management activities in the Minister's office, including increasing staff members' awareness of information management rules.
- Establish Service Alberta and the Provincial Archives of Alberta as monitors of departmental implementation with reporting requirements.
- Make all operational records schedules available for the public to view online to help establish openness, transparency and accountability in the management of government records.
- Ensure there are consequences for officials or departments found to have destroyed or handled records in contravention of the RM Regulation. No sanctions for contravening the RM Regulation existed.

The government publicly committed to implementing all of the recommendations.

Health Sector Preparedness for Mandatory Breach Provisions

Following a significant breach of Albertans' health information involving a stolen laptop, the Commissioner opened an investigation into breach reporting and notification in the health sector in 2014. Shortly thereafter, the Commissioner also wrote a letter to the former Minister of Health recommending mandatory breach reporting and notification provisions be considered for custodians subject to HIA.

During the course of this investigation, on May 14, 2014, Bill 12, the *Statutes Amendment Act*, was passed. This Act introduced amendments to HIA that included mandatory breach reporting and notification requirements, as well as new offence provisions for failing to report a privacy breach.

When the investigation report was published, the amendments were not in force; therefore, the investigation was not an investigation into compliance with HIA. Instead, the purpose was to analyze how breaches were being managed, tracked and reported in Alberta's health sector, and how prepared the sector was for mandatory breach reporting and notification.

Key findings from the investigation include:

- Large custodians – Alberta Health, Alberta Health Services and Covenant Health – generally had breach management frameworks in place, such as policies, procedures, education and training. However, many independent health professionals and smaller custodians had significant amounts of work to complete to establish breach response and reporting programs.
- Considerable training and education was necessary to ensure health custodians understand their breach reporting and notification obligations under the amended HIA.
- Tracking and monitoring breaches in the health sector has been inconsistent, making it difficult to estimate the number of breaches that occur, identify the underlying causes or assess the impact of mandatory breach reporting requirements.
- The Electronic Health Record Data Stewardship Committee (EHRDSC) had not met for two years which was a significant compliance issue identified in the investigation. The Committee is required by legislation and responsible for the governance of data made available through Alberta Netcare, the provincial electronic health record.

Review of the GoA's Travel and Expenses Policy

When the Government of Alberta announced its "Public Disclosure of Travel and Expenses Policy" in September 2012, it stated that it would ask the Information and Privacy Commissioner to review implementation of the policy. When the review was released in June 2015, the Commissioner said, "This policy is a positive step for Alberta, and compares well against similar initiatives in other jurisdictions."

That said, the OIPC made a number of recommendations based upon 11 best practice principles adapted from various standards for open government data initiatives. In particular, the OIPC recommended mandating proactive disclosure for certain types of information under legislation rather than through policy.

Offence Investigations

Since HIA was enacted in 2001, 2015-16 saw the most charges laid under the *Health Information Act* than any year previous. There were charges laid in four cases in connection with alleged unauthorized access to health information. In total, there have been charges laid in seven cases since 2001.

Under HIA, it is an offence for any person to knowingly gain or attempt to gain access to health information, or collect, use or disclose health information in contravention of HIA (section 107). Upon a breach report being submitted to the OIPC, the Commissioner may decide to launch an offence investigation after considering the circumstances of the case. If there is enough evidence to warrant charges, the OIPC will refer the matter to Crown prosecutors at Alberta Justice.

Of the four cases in which charges were laid in 2015-16, three are ongoing in the court system, while the fourth resulted in a conviction. The individual was convicted of knowingly accessing health information of seven people on 44 separate occasions in contravention of HIA.

Privacy Breach Reporting under HIA

Although mandatory breach reporting and notification provisions for health custodians have not yet been enacted, custodians voluntarily reported 129 privacy breaches to the OIPC. This represented a 70% increase from 2014-15 (76 total).

Incidents reported to the OIPC varied - from faxing errors to employee "snooping" of patient records - and these incidents can affect very few to many individuals.

In some cases, the Commissioner may open an offence investigation depending on the circumstances. As noted, the increase in offence investigations and charges resulting from those investigations was significant in 2015-16.

When a breach is reported to the OIPC, the office will work with the custodian and make any necessary recommendations to respond to the potential breach and to prevent similar incidents and encourage the custodian to report the incident to affected individuals, based on risk assessment. The decision to notify affected individuals rests with the custodian.

In May 2014, the government passed mandatory breach reporting and notification provisions but these amendments are not in force at this time.

Privacy Breach Reporting under FOIP

Unlike PIPA, there are no provisions for mandatory breach reporting and notification under the FOIP Act; and, unlike HIA, there are no amendments proposed to include such provisions. All privacy breaches reported to the OIPC by public bodies are voluntary reports. In 2015-16, there were 38 breach reports voluntarily filed by public bodies to the OIPC. This represented a slight decrease of 7% from 2014-15 (41).

The incidents that were reported included stolen property from vehicles, office thefts, employee "snooping", malware and phishing.

Privacy Breach Reporting under PIPA

Under PIPA, organizations must report privacy breaches to the Commissioner in situations where a reasonable person would consider there is a real risk of significant harm to an individual affected (section 34.1). This includes any loss, or unauthorized access or disclosure of personal information. The Commissioner has the power to require organizations to notify affected individuals when a privacy breach presents a real risk of significant harm (section 37.1).

In 2010, breach reporting and notification provisions in PIPA were enacted. Alberta became the first jurisdiction in Canada to have such provisions. Over the past five years, the OIPC has received approximately one breach report every five days under PIPA.

In 2015-16, there were 144 breach reports submitted to the OIPC, which represented a slight increase of 4% over 2014-15 (138).

A total of 125 breach decisions were issued by the Commissioner in 2015-16, which represented a 65% increase over 2014-15 (76).

Top Five Affected Industries
(Cases Opened)

- Retail
- Finance
- Insurance
- Mining, Oil and Gas
- Credit Unions

When a breach report is received, the OIPC:

- Determines whether the Commissioner has jurisdiction to review the matter
- Analyzes the circumstances of the situation as reported by the organization
- Reviews steps taken by the organization to reduce the risk of harm to individuals
- Reviews steps, if any, taken by the organization to notify affected individuals
- Reviews the organization's assessment of the risk of harm to individuals
- Decides whether the organization must notify affected individuals

There are three decisions the Commissioner may make:

- No jurisdiction
- No real risk of significant harm, organization not required to notify affected individuals
- Real risk of significant harm, organization required to notify affected individuals

Senior Executive Phishing Scam

One organization had its member list exposed due to a phishing scam. An unauthorized individual posed as the organization's CEO and duped an employee of the organization into disclosing names and email addresses of all 75,000 of the organization's members via email.

Uniquely, as part of its efforts to notify affected individuals, the organization in this situation issued a public notification and apology in a video posted on its website and to a social media site.

Several other similar phishing incidents where a fraudster posed as a senior executive from an organization to gain access to personal information were reported to the OIPC during 2015-16.

Association of Professional Engineers and Geoscientists of Alberta, P2015-ND-75

Hacking and Malware

A significant factor leading to the increased number of breaches reported to the office and real risk of significant harm decisions issued by the Commissioner was the prevalence of hacking and malware. These incidents can affect anywhere from just a few to millions of individuals.

Of the 125 breach decisions issued in 2015-16:

- 74% of decisions (92) involved a real risk of significant harm that required notification of affected individuals
- 15% of decisions (19) involved no real risk of significant harm
- 11% of decisions (14) found there was no jurisdiction

In one case, an organization had its systems compromised and hackers threatened to release the details of 37 million accounts for the organization's website.

Another case included an organization receiving a ransom demand from hackers who had compromised the organizations' computer systems affecting more than 130,000 individuals, including nearly 1,000 employees. The personal information was first accessed before the ransom demand was made. The hackers threatened to release the personal information online unless a ransom was paid.

In multiple cases, hackers installed malware on organizations' websites or gained unauthorized access to customer databases, specifically targeting financial and credit card information of customers. In one of these cases, it was a third party service provider that was hacked but the organization that reported the incident had control of the customer information that was affected, and the legal duty to report the incident to the OIPC.

In some of these hacking and malware incidents, organizations are based in the United States. Despite this, the Commissioner takes jurisdiction in these situations because the personal information in question is collected from Alberta residents while they are based in Alberta (via online transactions).

Avid Life Media Inc., P2015-ND-49

Enoch Casino Limited Partnership and River Cree Resort Limited Partnership, known as the River Cree Resort and Casino, P2016-ND-27

Infosat Communications GP Inc., P2015-ND-34

Well.ca, P2015-ND-45

Triple Flip Inc., P2015-ND-48

Simms Fishing Products, LLC, P2015-ND-58

Apple Leisure Group (AMResorts), P2015-ND-65

La Jolla Sport USA (O'Neill), MM Compound, Inc. (Metal Mulisha) and FMF Apparel, Inc. (FMF), P2015-ND-68

Park 'N Fly, P2016-ND-06

SRI Incorporated, P2016-ND-07

Credit Unions

Credit Union Central Alberta Ltd. was notified that paper records in its custody had been inadvertently stored in an unlocked basement room for several months during an office renovation. The records contained personal information of the organization's members.

PIPA requires the organization having "control" of the personal information to report the incident to the Commissioner. Therefore, in this case, considering Credit Union Central Alberta Ltd. was in "custody" of records for a number of its member credit unions, each credit union that controlled the records at issue reported the incident to the Commissioner.

In total, 22 separate credit unions notified the Commissioner about the incident. The Commissioner issued 22 breach notification decisions identifying a real risk of significant harm related to this one incident. The information related to each of these breach decisions is posted on the OIPC's website at www.oipc.ab.ca.

Unencrypted Mobile Devices

For more than a decade, the OIPC has been advising organizations to encrypt electronic devices, particularly mobile devices. Despite the widespread availability and use of encryption to protect sensitive information, one of the main causes leading to a real risk of significant harm decision by the Commissioner continues to be when unencrypted mobile devices containing personal information are lost or stolen.

In one case, although the organization's laptop was password protected and encrypted when it was stolen the laptop's password and encryption key were written down and stored with the laptop.

In another incident, the stolen laptop was password protected and encrypted, but the stolen USB sticks, which also contained personal information, were unencrypted.

In 2015-16, there were 10 such incidents where mobile devices were stolen. In some cases, the devices were password protected but unencrypted. In other cases, the devices were neither password protected nor encrypted.

Coca-Cola Company, P2015-ND-14

Sun Life Assurance Company of Canada, P2015-ND-35

Carson Integrated Ltd., P2015-ND-55

Suncor Energy Inc., P2015-ND-62

Affinity Psychology Group Corporation, P2015-ND-69

Kiewit Canada Corp., P2015-ND-72

Lyfe Kitchen Retail (Canada) Trust, P2015-ND-76

Acosta Canada Corporation, P2016-ND-01

Columbian Mutual Life Insurance Company, P2016-ND-05

Federated Insurance Company of Canada, P2016-ND-11

Summary of Significant Decisions

In 2015-16, the OIPC issued 64 Orders. Below is a brief summary of what were among the most significant of these decisions.

Use of Surveillance by Organizations Must Be Consistent with Purpose

An individual submitted a complaint to the OIPC claiming that the organization, a condominium corporation, had not installed signs notifying individuals of the extent of surveillance it carries out and the extent to which surveillance cameras are in use. He also complained that the organization's board reviews surveillance footage and uses information obtained from the footage to review bylaw infractions and to enforce compliance with the condominium bylaws.

The Adjudicator was satisfied that the organization's collection of personal information and notification to individuals met the requirements of PIPA. When residential condominiums collect personal information through surveillance in common areas it is reasonably understood that it is doing so to maintain security and to deter criminal acts. The Adjudicator was also satisfied that the increased use of surveillance, passed by the organization's board, was reasonable for the organization's stated purpose in order to address incidents of theft and criminal mischief that had occurred on the premises.

However, the Adjudicator did find that the organization's board had also used personal information in a manner not in accordance with its stated purpose for collection of personal information through surveillance. The complainant had written comments on a temporary notice the organization's board had posted in the elevator. After reviewing surveillance footage that identified the complainant, the organization issued a warning to him indicating he was "vandalizing" the notice. In its bylaws, the organization noted that the purpose for collection of personal information through surveillance was to deter "vandalism, theft, mischief, or a bylaw infraction". Considering the comments were scribbled on a temporary notice, the Adjudicator determined the incident could not be described as "vandalism", which would involve destruction of private or public property. The Adjudicator did consider whether the comments constituted "a bylaw infraction", but no evidence had been submitted by the organization to permit making such a determination.

Considering the organization's privacy policy did not refer to authorizing surveillance for the purpose of learning the identity of persons who write comments on temporary signage, the Adjudicator determined that the organization needed to obtain the complainant's consent for the collection of his personal information for this purpose. As it had not done so, the organization had contravened PIPA when it used the complainant's personal information to issue him a warning.

The organization was ordered to stop collecting and using personal information obtained from surveillance footage for purposes other than promoting and maintaining safety and security, unless notice under PIPA was provided for these other purposes.

Grandin Manor Ltd., Order P2016-02

Use of Personal Information in Public Bodies' Databases Inconsistent with Purpose for Collection

In two separate instances, personal information contained in databases managed by public bodies was collected, used or disclosed in contravention of the FOIP Act.

One complaint centred on the use of information in the Alberta Community Offender Management (ACOM) database. The public body argued that the complainant, a former employee of the public body, had consented to the use of information in this database because he had completed forms related to consenting to a criminal record check. However, the Adjudicator found that the complainant had not consented – expressly or by implication – to the use and/or disclosure of his personal information in the ACOM database.

The Adjudicator also found the purpose of the database was not to search information about employees or prospective employees; rather, the purpose was to track offenders serving in the community and to assist employees of the public body involved with these offenders. In this situation, the complainant's personal information was used to assess his honesty and integrity as an employee (to determine whether he had disclosed a criminal conviction which the public body believed he had). The Adjudicator held that this was not a purpose for which the information had been collected, nor was it consistent with this purpose.

The Adjudicator also determined there was no need to conduct an ACOM database search to determine the complainant's suitability for employment, as an element of the public body's operation of its program of running a prison because whether the complainant had a criminal record would have been disclosed through the mandatory criminal records check process (which indicated no criminal record) which every employee must undergo at the time of hiring. Based on these considerations, the Adjudicator decided the public body had no authority to use and/or disclose the complainant's personal information in the ACOM database.

The second complaint was about a search conducted by Alberta Human Services of the JOIN database, which was maintained by Alberta Justice and Solicitor General. Access was granted to Alberta Human Services only for the purpose of ensuring the safety of caregivers; however, the public body accessed the JOIN database to research the history of one of its employees. The public body argued the collection, use and disclosure of information was authorized for a variety of reasons, including conducting an investigation under the *Child and Youth Family Enhancement Act*.

The complainant submitted that the public body searched for and collected historical information regarding allegations that had not resulted in convictions, and had then used the collected information to make decisions regarding his employment, and disclosed the information to the Edmonton Police Service. He argued that the public body had no authority to conduct a search of the JOIN database and that the allegations being searched were not pertinent to his role in caring for youth in the care and custody of the public body.

The Adjudicator determined that the investigation did not relate to ensuring the safety of youth under the *Child and Youth Family Enhancement Act*. She also found that the complainant's personal information had not been collected, used or disclosed for any purposes for which a public body is permitted to collect, use, or disclose personal information under the FOIP Act.

Alberta Justice and Solicitor General, Order F2015-27

Alberta Human Services, Order F2015-42

Custody and Control of Records under PIPA and the FOIP Act

The applicant made requests to an organization under PIPA, and a public body under the FOIP Act for records related to the "place, care, and termination" of his son at a child care agency.

In response to the request, the public body provided some records in its custody, but took the position that it had no control over the organization's records. The organization initially ignored the request because it believed it did not have to respond.

The Adjudicator reviewed the contract between the public body and the organization and determined that the public body had control over any recorded information created or received by the organization in the performance of its duties under the contract. The Adjudicator also found that the public body had the right to demand the information from the organization through its contractual agreement. Therefore, if responsive records to the request had not been produced, but existed, and if they were located at the organization, then the public body would have control over them within the terms of the FOIP Act. Based on these determinations, the public body was ordered to conduct a new search for responsive records and to prepare a new response to the applicant.

With regard to the organization, the Adjudicator held that it had conducted an adequate search for records, and that it did not have an obligation to look for certain records that were under the control of the public body and thus subject to the FOIP Act. The organization had, however, failed to meet its time limit to respond to the request.

Watch My Grow Agency, F2015-08

Northwest Alberta Child and Family Services Authority Region 8, F2015-21

Records Claimed to be Privileged

The applicant requested information about himself from Alberta Justice and Solicitor General. The public body withheld responsive records it had located, relying on section 27(1) of the FOIP Act. The subject matter of the information at issue in this case was the applicant's suitability as a police investigator and witness for the Alberta Crown Prosecution Service. The Crown Prosecution Service had shared the information with the Calgary Police Association.

After analyzing the sequence of events, the Adjudicator found that the information at issue, claimed by the public body to be protected by solicitor-client privilege, had not been created in the context of a solicitor-client relationship between the Alberta Crown Prosecution Service and the Calgary Police Service; the Alberta Crown Prosecution Service had been communicating a decision regarding the applicant's suitability as a witness, rather than giving advice.

The Adjudicator also determined that there was no common interest between the Calgary Police Service and Calgary Police Association; therefore, when the Alberta Crown Prosecution Service shared information it claimed to be privileged with the Calgary Police Association it lost any status it may have had as subject to solicitor-client privilege.

Further, the Adjudicator found that sections 27(1)(b) and 27(1)(c) had not been properly applied. While some portions of these provisions were met, the information at issue essentially involved the communication of a decision, rather than the provision of a legal service. As well, the Adjudicator commented that sections 27(1)(b) and 27(1)(c) cannot, by reference to their wording, be sensibly applied to legal advice, since information "in relation to legal advice" cannot be the advice itself. The Adjudicator also rejected the public body's claim of settlement negotiation privilege. The public body was ordered to disclose the records to the applicant.

Alberta Justice and Solicitor General, F2015-31

Deemed Refusals to Respond to Applicants

The only issue in these inquiries was the time limit for responding to the applicants' access requests.

In each case, the public bodies acknowledged that they had not yet responded to the applicants. One public body noted a backlog of files waiting to be processed, while both public bodies indicated that staff shortages made it difficult to respond to the requests within the time limits set out in the FOIP Act. The complexity of the request was also noted in one instance.

In each case, the Adjudicators recognized the constraints faced by the public bodies. However, it ordered the public bodies to respond to the applicants' access requests, as the time limits set out in the FOIP Act are mandatory.

Alberta Justice and Solicitor General, F2016-04, F2016-05, F2016-06 and F2016-07

Alberta Environment and Parks, F2016-08

Judicial Reviews and Other Court Decisions

University of Calgary v. JR

2015 ABCA 118, which reversed 2013 ABQB 652, which upheld an Adjudicator's Notice to Produce Records alleged to be subject to solicitor-client privilege

An individual, a former employee of the University of Calgary, made an access request for information held by various other employees of the public body, a Wellness Centre and a doctor associated with the Wellness Centre. The public body provided some of the information, but withheld other information under various exceptions to disclosure contained in the FOIP Act, including section 27(1)(a) (solicitor-client privilege). The individual requested that the Commissioner review the public body's decisions to withhold information.

In an inquiry under the FOIP Act, the public body chose not to provide the Adjudicator with a copy of the records for which it claimed that solicitor-client privilege applied, in accordance with the *Solicitor-Client Privilege Adjudication Protocol* of the Commissioner's Office.

In accordance with the *Protocol*, the Adjudicator requested additional argument and evidence from the public body so that he could decide whether it properly applied section 27(1)(a) to the records. The public body provided a minimal amount of additional information, which was insufficient for the Adjudicator to decide the issue. The Adjudicator sent the public body a notice under section 56(2) of the FOIP Act to produce the records so that he could decide whether the public body had the authority to withhold those records.

The public body applied for judicial review of the Adjudicator's Notice to Produce Records. The Court held that the standard of review was correctness, and that the FOIP Act gave the Adjudicator authority to issue a Notice to Produce in relation to records alleged to be subject to solicitor-client privilege. The Court also held that recourse to the Notice to Produce was necessary in this case to verify the claim for privilege. The Court upheld the Adjudicator's decisions as being correct.

On appeal by the public body, the Court of Appeal allowed the appeal and reversed the lower Court's decision. The Court of Appeal held, at para. 49:

> [49] Applying *Blood Tribe*'s direction to the language of section 56(3) leads unavoidably to the conclusion that it does not authorize the Commissioner or her delegate to order a public body to produce to her records over which it has asserted solicitor-client privilege. Section 56(3) does not clearly, explicitly and specifically authorize infringement of solicitor-client privilege. Rather, it merely provides that a public body must turn over records, despite any privilege of the law of evidence that exists. To convert that general statement into an authorization for demanding that a public body do so where the privilege claimed is solicitor-client privilege, an impermissible inference must be drawn, premised upon solicitor-client privilege having been implicitly captured by the general language negating "any privilege of the law of evidence". This is precisely the sort of statutory construction that *Blood Tribe* precludes.

The Commissioner has obtained leave to appeal the Court of Appeal's decision to the Supreme Court of Canada.

Edmonton (City) v. Alberta (Information and Privacy Commissioner)

2015 ABQB 246 – Judicial Review of Order F2013-53

An individual made a request under the FOIP Act to the City of Edmonton for access to all records relating to herself or her property for a certain time period. The public body informed the Applicant that her request was for general information, not personal information, and was therefore subject to a $25 initial fee.

The applicant requested a review of the public body's decision to charge the fee, arguing that her request was for personal information. The applicant also requested a review of the public body's response, alleging that the public body failed to comply with its duty to assist and with the timelines of the FOIP Act.

At inquiry, the Adjudicator found that the public body did not meet the timelines required under the FOIP Act, and that it did not meet its duty to assist the applicant because it failed to properly define her request. The Adjudicator also determined that the applicant's request was a request for bylaw complaints about the applicant. As such, it was a request for "personal information" and is therefore not subject to the $25 initial fee. Finally, the Adjudicator found that the public body did not consider all of the relevant factors in withholding information in the responsive records under section 17 of the FOIP Act. The Adjudicator ordered the public body to consider all relevant circumstances in making the decision to disclose or withhold personal information in the responsive records.

On judicial review by the public body, the main issue before the Court was the Adjudicator's interpretation that "personal information" in the FOIP Act included bylaw complaints about the applicant, and whether that interpretation was contrary to the interpretation of "personal information" set out by the Court of Appeal in *Leon's Furniture Limited v. Alberta (Information and Privacy Commissioner)*, 2011 ABCA 94, and was therefore unreasonable. The Court of Appeal in Leon's held that information related to an object or property was not "personal information" under PIPA because it was not information "about an individual".

The Court found that it was reasonable for the Adjudicator to determine that bylaw complaints were "personal information" under the FOIP Act. The Court said, at para. 79:

> [79] The interpretation of "personal information" that includes bylaw complaints about an individual, such as the Applicant, is consistent with the broad approach to interpreting privacy legislation mandated by the Supreme Court and other authorities. Since the information directly bears on an individual's preservation of her interests in property as against the coercive powers of the City, the propriety of a broad approach to the interpretation of "personal information" is further supported.

The Court held that the Adjudicator's decisions fell within the range of possible, acceptable outcomes and were defensible in respect of both the facts and the law. The Court also said that the Adjudicator's reasons were transparent and intelligible, and that the reasons justified the decisions made.

As the public body had not established that the Adjudicator's decisions were unreasonable, the Court dismissed the public body's judicial review application.

The public body has appealed the Court's decision.

ABC Benefits Corporation v. Alberta (Information and Privacy Commissioner)

2015 ABQB 662 – Judicial Review of Order F2013-47

The Applicant requested a copy of the agreement between Alberta Health and Alberta Blue Cross (ABC) under which ABC administers the provincial drugs plan. The public body produced the agreement but withheld some information under section 16 (disclosure harmful to business interests) and section 25 (disclosure harmful to economic and other interests) of the FOIP Act.

At inquiry, the Adjudicator found that some of the information did not meet the requirements of section 16(1)(a), as it could not be said to be information belonging to ABC. The Adjudicator also determined that none of the information in the agreement could be said to have been supplied by ABC as required by section 16(1)(b), and was therefore not subject to section 16 for that reason as well. Having made that finding, the Adjudicator said that she need not address whether the information met the requirements of section 16(1)(c) at this time.

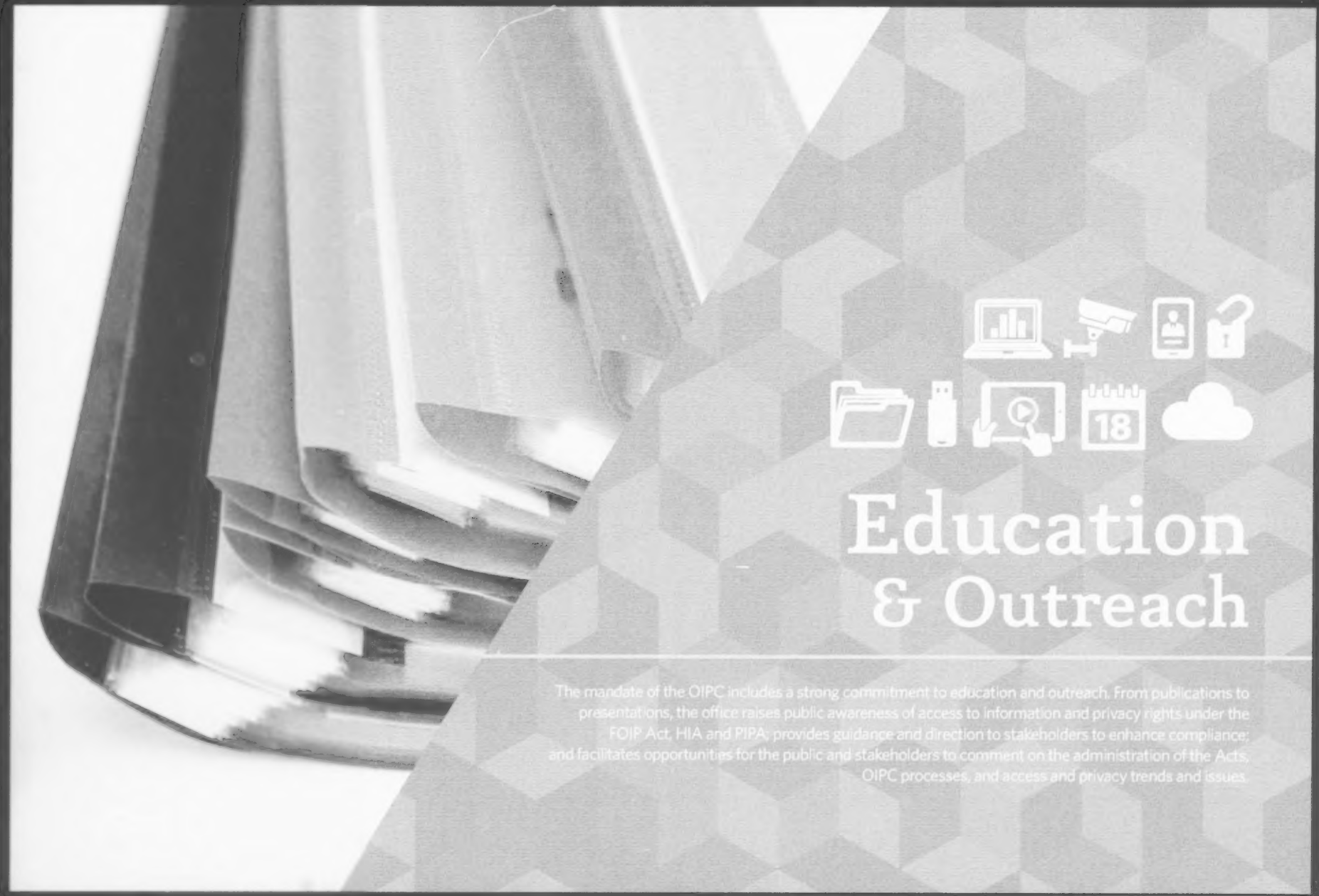
The Adjudicator further found that the public body had not established that disclosure of the information withheld from the applicant under section 25 could result in harm within the terms of section 25. The Adjudicator ordered the public body to disclose the agreement in its entirety.

On judicial review by ABC, the Court held that the Adjudicator's decision that the evidence did not meet the test under section 25 was reasonable.

However, the Court held that the Adjudicator's decision that the withheld information was not "supplied" by ABC under section 16(1)(b) was unreasonable because:

- The Adjudicator's "reasoning process was flawed and has been overtaken by the Court of Appeal's comments in *Imperial Oil* [*Imperial Oil Limited v. Alberta (Information and Privacy Commissioner)*, 2014 ABCA 231], at para. 83, that information does not lose the statutory protection from disclosure just because it ends up in an agreement that had been negotiated." (para. 72)
- The Adjudicator unreasonably failed to address ABC's evidence about the basis for calculating the rates and fees in the agreement (para. 73)
- *Imperial Oil*, at para. 70 noted that section 16(1)(a) "does not necessarily require ownership of the information in the strict sense. It is the information as applied to the business of the third party that would be 'of the third party'." (para. 75)

The Court remitted the matter to the Commissioner to determine whether the withheld information met the criteria of section 16(1)(b) and section 16(1)(c) of the FOIP Act.



Education & Outreach

The mandate of the OIPC includes a strong commitment to education and outreach. From publications to presentations, the office raises public awareness of access to information and privacy rights under the FOIP Act, HIA and PIPA; provides guidance and direction to stakeholders to enhance compliance; and facilitates opportunities for the public and stakeholders to comment on the administration of the Acts, OIPC processes, and access and privacy trends and issues.

OIPC Website Revamp

A highly anticipated new OIPC website was unveiled in December 2015. In addition to a new look and feel, the functionality and content were revamped with the intent to ensure visitors could find what they were looking for within a couple of clicks. In particular, the format of the new website was designed to help members of the public who may be seeking to submit a request for review or complaint to find the most pertinent information on the homepage.

Resources Published in 2015-16

- Motor Vehicle Dealership Test Drives: Collection, Use and Disclosure of Driver Licence Information (April 2015)
- Access to Information Laws in Alberta (June 2015)
- Privacy Laws in Alberta (June 2015)
- Is a Bring Your Own Device (BYOD) Program the Right Choice for Your Organization? Privacy and Security Risks of a BYOD Program (August 2015)
- Kids' Privacy Sweep Lesson Plan (September 2015)
- Privacy Impact Assessment Guidelines for Insurers Looking to Implement Usage-Based Insurance Programs in Alberta (January 2016)
- Advisory for Ransomware (March 2016)

Presentations, Forums and Workshops

In 2015-16, the Commissioner and OIPC staff participated in 74 presentations, training sessions and speaking engagements. These local and national events provide an opportunity for the office to promote its educational mandate, increase awareness about access and privacy issues, and share the office's experiences.

School at the Legislature

The Legislative Assembly of Alberta's School at the Legislature program, in which the OIPC continued to participate, provides a great opportunity to connect OIPC staff with young Albertans to discuss access and privacy.

University of Alberta's Access and Privacy Conference: 20 Years of the FOIP Act

The 2015 Access and Privacy Conference hosted by the University of Alberta's Faculty of Extension took on special meaning as the province celebrated 20 years of the FOIP Act. Among other opportunities to recognize 20 years, the conference included a panel discussion with former Commissioners Robert C. Clark and Franklin J. Work, Q.C., and current Commissioner Jill Clayton.

Committee support continued to be provided by the OIPC for the conference.

Data Privacy Day

Internationally recognized, January 28 marks Data Privacy Day to promote the protection of personal information.

Throughout 2015-16, there was a significant increase in attention paid to privacy breaches, not to mention an increase in privacy breach reports submitted to the OIPC. To respond to this, the OIPC's 2016 Data Privacy Day event in Calgary focused on the theme of "Breach Response and Reporting".

The morning forum included speakers from the University of Calgary, City of Calgary and Alberta Health Services discussing a wide range of topics, including trends in legislation, big data analytics and its effects on privacy, IT security and breach prevention, and breach response and reporting.

The afternoon session provided an opportunity to unveil the OIPC's new workshop offering on breach response and reporting. This workshop was developed, in part, to help the health sector prepare for upcoming mandatory breach reporting and notification provisions to be enacted under HIA. However, the workshop provides general guidance for all stakeholders from the public, health and private sectors.

The Commissioner also wrote an op-ed published in the Calgary Herald and Edmonton Journal for Data Privacy Day on the topic of privacy breaches to emphasize the importance of valuing and protecting personal information.

Right to Know Week Forums

Right to Know Day is internationally recognized annually on September 28 to generate awareness about an individual's right to access public information and to promote freedom of information as a cornerstone to democracy. Importantly, in November 2015, the United Nations Educational, Scientific and Cultural Organization (UNESCO) proclaimed September 28 as the "International Day for the Universal Access to Information".

The timing for Right to Know Week coincided with the FOIP Act's 20th year. On October 1, 1995, the FOIP Act came into force in Alberta; fast forward 20 years when the OIPC hosted its Right to Know Week Forum in Edmonton on October 1, 2015. The OIPC also held an event to recognize the public's right to know on September 29 in Calgary.

Beyond providing an opportunity to celebrate 20 years of the public's right to know in Alberta, the OIPC's 2015 forums included a presentation by Sean Holman, Assistant Journalism Professor at Mount Royal University and access to information advocate, who explored the state of freedom of information in Alberta, as well as the amount of cultural and political support – or lack thereof – for expanding that freedom. OIPC staff members Mary Golab and Catherine Taylor also presented on the Magna Carta, which celebrated 800 years in 2015 and laid the foundation for access to information and the public's right to know. In Calgary, there was a Chat with the Commissioner session and, in Edmonton, the City of Edmonton presented on its Open City Initiative.

PIA and Breach Workshops

Following the Breach Response and Reporting Workshop at the Data Privacy Day event in Calgary, the OIPC hosted the workshop in Edmonton. The workshop included discussion on developing a privacy breach response plan, establishing a breach response team, successful strategies in remediating privacy breaches and issues around identifying affected individuals and notification challenges. With the prevalence of privacy breaches being reported to the OIPC and anticipated mandatory breach reporting and notification provisions under HIA, the OIPC intends to make this workshop part of its regular educational offering for public bodies, custodians and organizations.

The OIPC also continued to provide PIA training. These workshops assist stakeholders in reviewing the impact that a new project may have on individual privacy. The workshops cover the essentials of a PIA. Only custodians under HIA are required by law to submit a PIA for review by the office; however, the office highly recommends public bodies

and private sector organizations consider completing PIAs to help mitigate risks to personal information in new initiatives or when reviewing existing programs that involve the collection, use or disclosure of personal information.

Usage-Based Insurance PIA Training

In April 2016, insurers operating in Alberta could begin offering their customers usage-based insurance (UBI). UBI is a type of automobile insurance where insurers consider additional rating factors to determine the level of insurance premiums to be paid by policy holders. For UBI programs to operate, they involve the collection, use and disclosure of information pertaining to the operation of a motor vehicle by individuals.

Leading up to the implementation of this program in Alberta, the Superintendent of Insurance made it a requirement that insurance providers must complete a PIA and submit it to the OIPC for review and acceptance prior to offering the product to its customers. The OIPC, in turn, developed *Privacy Impact Assessment Guidelines for Insurers Looking to Implement Usage-Based Insurance Programs* in Alberta in preparation for the requirement placed upon insurers.

In March 2016, the Office of the Superintendent of Insurance invited the OIPC to present to a group of representatives from insurance organizations operating in Alberta. The purpose of the half-day session was to highlight the requirements for insurers to prepare PIAs ahead of the implementation of UBI products in the province. The session discussed general requirements under PIPA and offered specific guidance for the preparation of PIAs to demonstrate that insurers have considered the requirements of PIPA and have made a reasonable effort to protect privacy and mitigate risk when implementing UBI products.

As of March 31, 2016, three PIAs for automobile UBI products had been submitted by insurance organizations and were accepted by the OIPC. Acceptance of a PIA is not approval. It simply reflects the opinion of the office that the privacy requirements under the Act have been considered, and the organization has made a reasonable effort to protect privacy.

Genetic Testing Panel

The Commissioner moderated a panel on the topic of "Health, Privacy and Genetics" at the Privacy and Access 20/20 Conference in Vancouver hosted by the Information and Privacy Commissioner for British Columbia.

The session explored the privacy implications of expanded collection and use of genomic data in the public and private sectors, and contemplated the legal, ethical and policy solutions to be considered with rapid advances in technologies in this area.

The panel included experts in health law and policy, a representative from the insurance industry and a civil liberties advocate.

Collaboration with Other Jurisdictions

Guidance on Bring Your Own Device Programs for Private Sector Organizations

In partnership with the Office of the Privacy Commissioner of Canada and the Office of the Information and Privacy Commissioner for British Columbia, guidelines were published to address what organizations should consider when determining whether to implement bring your own device (BYOD) programs.

BYOD programs blur the lines between professional and personal lives of employees, and create issues associated with consumers' personal information, the guidelines note. To help organizations assess risk, the guidelines focus on 13 privacy and security considerations for making a decision on incorporating a BYOD program.

Joint Resolution on Government Information Sharing and Statement on the Duty to Document

In January 2016, Canada's Information and Privacy Commissioners and Ombudspersons released two documents.

First, a joint resolution on *Protecting and Promoting Canadians' Privacy and Access Rights in Information Sharing Initiatives* called on all levels of government to consider certain actions prior to embarking on information sharing programs aimed at improving government services. This was signed by all Information and Privacy Commissioners and Ombudspersons across Canada.

Second, a joint statement was issued by Information Commissioners and Ombudspersons on the duty to document. This statement expressed the regulators' concerns about the trend towards no records responses to access to information requests. As a result, Information Commissioners and Ombudspersons called on their respective governments to create a legislated duty requiring public entities to document matters related to their deliberations, actions and decisions.

Global Privacy Sweep and Lesson Plan

The OIPC was one of 29 international information and privacy regulators to participate in the Global Privacy Enforcement Network's (GPEN) Privacy Sweep, which focused on children's online privacy in 2015.

Of the 1,494 websites and apps analyzed around the globe, 67% were found to collect children's personal information and 50% shared information with other organizations.

The OIPC reviewed 20 websites and apps from Alberta-based organizations. Encouraging in the data from Alberta was that 14 of the 20 websites did not collect individually identifying personal information except for website cookies and IP addresses.

In preparing for the results, the OIPC partnered with the Office of the Privacy Commissioner of Canada to release the *Kids' Privacy Sweep Lesson Plan* for students in Grades 7 and 8. The lesson plan was released concurrently with the privacy sweep results.

The purpose of the lesson plan was to help students:

- Gain an appreciation of what "personal information" is in the context of privacy laws
- Become aware of how and why websites and apps collect personal information
- Better understand privacy policies and privacy communications to make informed choices about the websites they visit and the apps they use

Media Awareness

Traditional Media

The OIPC received 105 media requests. This represented a slight decrease of 13% from 2014-15 (120).

The topic that received the most media attention throughout the year was the investigation into the alleged improper destruction of records by Alberta Environment and Sustainable Resource Development – colloquially known as the "shredding" investigation – that was launched in the wake of the May 2015 provincial election. There was plenty of public and media interest in the investigation both when it was launched and again when the investigation report was released in January 2016. The investigation was completed jointly with the Office of the Public Interest Commissioner.

Other topics that received considerable media attention in 2015-16 included:

- The OIPC's involvement in the Global Privacy Enforcement Network's Privacy Sweep of online applications and websites that target children resulted in a number of calls from media. Not only were results reiterated to media, but the office was able to promote its Privacy Sweep Lesson Plan for students in Grades 7 and 8 that was developed in partnership with the Office of the Privacy Commissioner of Canada and released with the privacy sweep results.
- A privacy breach at AHS that initially resulted in a number of employees being reprimanded received plenty of media attention in Calgary. The message from the office as it relates to health information "snooping" was reiterated: With access to health information comes great responsibility for health professionals and administrators to protect the privacy of patients.
- The office's investigation report on the health sector's preparedness for breach reporting and notification requirements under HIA also received significant attention. The investigation found that large custodians were generally prepared and had processes in place; meanwhile, smaller custodians in many cases had plenty of work to do to prepare for the provisions. In addition, the office noted the non-compliance issue at Alberta Health where the Electronic Health Record Data Stewardship Committee, required by legislation and responsible for overseeing stewardship of data made available through Netcare, had not met for more than two years.
- An off-duty member of the Calgary Police Service had police notebooks containing personal information stolen from his personal vehicle (among other property stolen that belonged to the Calgary Police Service). The office's response to media requests focused on the absence of mandatory breach reporting and notification requirements under the FOIP Act, but did recognize the Calgary Police Service's efforts in attempting to notify affected individuals.

There was a significant reduction in the number of news releases issued by the office in 2015-16 due to a change in process for releasing Orders that took effect April 1, 2015. Rather than issuing a news release for each Order, which had been the OIPC's practice since April 1998, the office instead posts the Order on the website and notifies the public via Twitter.

Social Media

The OIPC issued 244 tweets in 2015-16, including all replies and retweets, which was a significant reduction from 344 tweets issued in 2014-15. In 2014-15, the OIPC was establishing its social media presence and, to do so, tweeted more frequently to gain an audience.

The three topics that received the most attention on social media were:

- The release of the records management investigation report. Unlike traditional media where both the announcement of the investigation and release of the report had a similar amount of coverage, on social media the release of the report gained more than two times the coverage.
- The *Advisory for Ransomware* the office published in March 2016 was the most viewed and retweeted resource.
- The news release regarding the results of the Global Privacy Enforcement Network's Privacy Sweep and the office's involvement.

The OIPC's *Review of the Personal Information Protection Act: Submission to the Standing Committee on Alberta's Economic Future* also received a number of views through social media and resulted in coverage by traditional media despite not having an associated news release.

Robert C. Clark Award

Introduced in 2013, the Robert C. Clark Award, named after Alberta's first Information and Privacy Commissioner, recognizes an individual, group or organization that has contributed significantly to advancing access to information in Alberta.

Bonnie Nelson received the award in 2015 for her leadership in promoting open data at Alberta Environment and Sustainable Resource Development (now known as Alberta Environment and Parks). Her efforts included managing the implementation of the first routine disclosure program for Alberta Environment, which helped pave the way for other open data initiatives in the province.

An independent, three-person panel made up of subject matter experts with extensive experience in the field reviewed the nominations and selected the award recipient. The selection panel members were:

- Catherine Tully, Information and Privacy Commissioner for Nova Scotia
- Ann Cavoukian, Executive Director of the Privacy and Big Data Institute at Ryerson University and former Information and Privacy Commissioner of Ontario
- Alasdair S. Roberts, Professor of Public Affairs at the Truman School of Public Affairs at the University of Missouri

Financial Statements

Independent Auditor's Report 56
Statement of Operations 57
Statement of Financial Position 58
Statement of Changes in Net Debt 59
Statement of Cash Flows 60
Notes to the Financial Statements 61
Schedule 1 - Salary and Benefits Disclosure 65
Schedule 2 - Allocated Costs 66

AUDITOR GENERAL *Alberta*

Independent Auditor's Report

To the Members of the Legislative Assembly:

Report on the Financial Statements

I have audited the accompanying financial statements of the Office of the Information and Privacy Commissioner, which comprise the statement of financial position as at March 31, 2016, the statements of operations, change in net debt and cash flows for the year then ended, and a summary of significant accounting policies and other explanatory information.

Management's Responsibility for the Financial Statements

Management is responsible for the preparation and fair presentation of these financial statements in accordance with Canadian public sector accounting standards, and for such internal control as management determines is necessary to enable the preparation of financial statements that are free from material misstatement, whether due to fraud or error.

Auditor's Responsibility

My responsibility is to express an opinion on these financial statements based on my audit. I conducted my audit in accordance with Canadian generally accepted auditing standards. Those standards require that I comply with ethical requirements and plan and perform the audit to obtain reasonable assurance about whether the financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditor's judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

I believe that the audit evidence I have obtained is sufficient and appropriate to provide a basis for my audit opinion.

Opinion

In my opinion, the financial statements present fairly, in all material respects, the financial position of the Office of the Information and Privacy Commissioner as at March 31, 2016, and the results of its operations, its remeasurement gains and losses, its changes in net debt and its cash flows for the year then ended in accordance with Canadian public sector accounting standards.

Original signed by
Merwan N. Saher, FCPA, FCA

Auditor General
July 13, 2016
Edmonton, Alberta

Office of the Information and Privacy Commissioner

Statement of Operations

Year ended March 31, 2016

	2016 Budget	2016 Actual	2015 Actual
Revenues			
Prior Year Expenditure Refund	$ -	$ 25,004	$ 3,024
Other Revenue	-	1,745	291
	-	26,749	3,315
Expenses - Directly Incurred (Note 3a)			
Salaries, Wages, and Employee Benefits	$ 5,640,141	$ 5,465,185	$ 5,183,369
Supplies and Services	1,203,199	1,373,261	1,587,093
Amortization of Tangible Capital Assets	74,000	79,553	83,876
Total Expenses	6,917,340	6,917,999	6,854,338
Net Operating Results	$ (6,917,340)	$ (6,891,250)	$ (6,851,023)

The accompanying notes and schedules are part of these financial statements.

Financial Statements

Office of the Information and Privacy Commissioner

Statement of Financial Position

As at March 31, 2016

	2016	2015
Financial Assets		
Cash	$ 100	$ 100
Accounts Receivable	3,281	3,271
	$ 3,381	$ 3,371
Financial Liabilities		
Accounts Payable and Accrued Liabilities	$ 403,737	$ 408,482
Accrued Vacation Pay	512,231	537,555
	$ 915,968	$ 946,037
Net Debt	$ (912,587)	$ (942,666)
Non-Financial Assets		
Tangible Capital Assets (Note 4)	$ 122,967	$ 202,520
Prepaid Expenses	7,035	295
	$ 130,002	$ 202,815
Net Liabilities	$ (782,585)	$ (739,851)
Net Liabilities at Beginning of Year	(739,851)	(672,118)
Net Operating Results	(6,891,250)	(6,851,023)
Net Financing Provided from General Revenues	6,848,516	6,783,290
Net Liabilities at End of Year	$ (782,585)	$ (739,851)

The accompanying notes and schedules are part of these financial statements.

Office of the Information and Privacy Commissioner

Statement of Changes in Net Debt

Year ended March 31, 2016

	2016	2015
Annual Deficit	$ (6,891,250)	$ (6,851,023)
Acquisition of Tangible Capital Assets	-	(18,651)
Amortization of Tangible Capital Assets	79,553	83,876
Change in Prepaid Expenses	(6,740)	610
Net Financing Provided from General Revenue	6,848,516	6,783,290
Decrease (Increase) in Net Debt for the Year	30,079	(1,898)
Net Debt, Beginning of Year	(942,666)	(940,768)
Net Debt, End of Year	$ (912,587)	$ (942,666)

The accompanying notes and schedules are part of these financial statements.

Financial Statements

Office of the Information and Privacy Commissioner

Statement of Cash Flows

Year ended March 31, 2016

	2016	2015
Operating Transactions		
Net Operating Results	$ (6,891,250)	$ (6,851,023)
Non-Cash Items Included in Net Operating Results		
Amortization of Tangible Capital Assets	79,553	83,876
Loss on Disposal of Tangible Capital Assets	-	-
	(6,811,697)	(6,767,147)
(Increase) in Accounts Receivable	(10)	(3,237)
Decrease (Increase) in Prepaid Expenses	(6,740)	610
Increase (Decrease) in Accounts Payable	(30,069)	5,135
Cash Applied to Operating Transactions	(6,848,516)	(6,764,639)
Capital Transactions		
Acquisition of Tangible Capital Assets	-	(18,651)
Financing Transactions		
Net Financing Provided from General Revenues	6,848,516	6,783,290
Cash, Increase (Decrease)	-	-
Cash, Beginning of Year	100	100
Cash, End of Year	$ 100	$ 100

The accompanying notes and schedules are part of these financial statements.

Office of the Information and Privacy Commissioner

Notes to the Financial Statements

Year ended March 31, 2016

Note 1 Authority

The Office of the Information and Privacy Commissioner operates under the authority of the *Freedom of Information and Protection of Privacy Act*. General Revenues of the Province of Alberta fund both the cost of operations of the Office of the Information and Privacy Commissioner and the purchase of tangible capital assets. The all-party Standing Committee on Legislative Offices reviews and approves the office's annual operating and capital budgets.

Note 2 Purpose

The Office of the Information and Privacy Commissioner provides oversight on the following legislation governing access to information and protection of privacy:

Freedom of Information and Protection of Privacy Act
Health Information Act
Personal Information Protection Act

The major operational purposes of the Office of the Information and Privacy Commissioner are:

- To provide independent reviews of decisions made by public bodies, custodians and organizations under the Acts and the resolution of complaints under the Acts;
- To advocate protection of privacy for Albertans; and
- To promote openness and accountability for public bodies.

Note 3 Summary of Significant Accounting Policies and Reporting Practices

These financial statements are prepared in accordance with Canadian public sector accounting standards, which use accrual accounting. The office has adopted PS 3450 Financial Instruments. The adoption of this standard has no material impact on the financial statements of the office, which is why there is no statement of remeasurement gains and losses.

Other pronouncements issued by the Public Sector Accounting Board that are not yet effective are not expected to have a material impact on future financial statements of the office.

Office of the Information and Privacy Commissioner

Notes to the Financial Statements *(continued)*

Year ended March 31, 2016

Note 3 Summary of Significant Accounting Policies and Reporting Practices (continued)

a) Expenses

The office's expenses are either directly incurred or incurred by others:

Directly incurred

Directly incurred expenses are those costs incurred under the authority of the office's budget as disclosed in Schedule 2.

Pension costs included in directly incurred expenses comprise employer contributions to multi-employer plans. The contributions are based on actuarially determined amounts that are expected to provide the plans' future benefits.

Incurred by others

Services contributed by other entities in support of the office's operations are not recognized and are disclosed in Schedule 2.

b) Tangible capital assets

Tangible capital assets are recorded at historical cost less accumulated amortization. Amortization begins when the assets are put into service and is recorded on a straight-line basis over the estimated useful lives of the assets. The threshold for tangible capital assets is $5,000 except major enhancements to existing systems is $250,000 and new systems development is $100,000.

c) Net debt

Net debt indicates additional cash that will be required from General Revenues to finance the office's cost of operations to March 31, 2016.

Office of the Information and Privacy Commissioner

Notes to the Financial Statements *(continued)*

Year ended March 31, 2016

Note 4 Tangible Capital Assets

	Office equipment and furniture	Computer hardware and software	Total
Estimated Useful Life	5 years	5 years	
Historical Cost			
Beginning of Year	$ 255,380	$ 413,934	$ 669,315
Additions	-	-	-
Write-Downs	(172,062)	(53,734)	(225,796)
	$ 83,318	$ 360,200	$ 443,518
Accumulated Amortization			
Beginning of Year	$ 214,498	$ 252,297	$ 466,795
Amortization Expense	21,319	58,234	79,553
Effect of Write-Downs	(172,062)	(53,734)	(225,796)
	$ 63,756	$ 256,796	$ 320,552
Net Book Value at March 31, 2016	$ 19,562	$ 103,404	$ 122,967
Net Book Value at March 31, 2015	$ 40,882	$ 161,638	$ 202,520

Office of the Information and Privacy Commissioner

Notes to the Financial Statements *(continued)*

Year ended March 31, 2016

Note 5 Defined Benefit Plans

The Office participates in the multiemployer pension plans: Management Employees Pension Plan, Public Service Pension Plan and Supplementary Retirement Plan for Public Service Managers. The expense for these pension plans is equivalent to the annual contributions of $808,135 for the year ended March 31, 2016 (2015 - $721,657).

At December 31, 2015, the Management Employees Pension Plan reported a surplus of $299,051,000 (2014 surplus $75,805,000) and the Public Service Pension Plan reported a deficiency of $133,188,000 (2014 deficiency $803,299,000). At December 31, 2015, the Supplementary Retirement Plan for Public Service Managers had a deficiency of $16,305,000 (2014 deficiency $17,203,000).

The Office also participates in a multiemployer Long Term Disability Income Continuance Plan. At March 31, 2016, the Management, Opted Out and Excluded Plan reported an actuarial surplus of $29,246,000 (2015 surplus $32,343,000). The expense for this plan is limited to employer's annual contributions for the year.

Note 6 Contractual Obligations

Contractual obligations are obligations of the Office to others that will become liabilities in the future when the terms of those contracts or agreements are met.

	2016	2015
Obligations under operating leases and contracts	$ 27,463	$ 11,958

Estimated payment requirements for each of the next three years are as follows:

	Total
2016-17	$ 13,175
2017-18	9,496
2018-19	4,792
	$ 27,463

Office of the Information and Privacy Commissioner

Notes to the Financial Statements *(continued)*

Note 7 Approval of Financial Statements

These financial statements were approved by the Information and Privacy Commissioner.

Schedule 1 - Salary and Benefits Disclosure

Year ended March 31, 2016

	2016				2015
	Base Salary [a]	Other Cash Benefits	Other Non-cash Benefits [b][c]	Total	Total
Senior Official					
Information and Privacy Commissioner	$ 197,672	$ -	$ 60,849	$ 258,521	$ 254,665

[a] Base salary includes pensionable base pay.
[b] Other non-cash benefits include the government's share of all employee benefits and contributions or payments made on behalf of employee, including pension, supplementary retirement plan, health care, dental coverage, group life insurance, short and long term disability plans, health spending account, conference fees, and professional memberships and tuition fees.
[c] Other non-cash benefits for the information and privacy commissioner includes $8,811 (2015: $7,499) being the lease, fuel, insurance and maintenance expenses for an automobile provided by the office.

Office of the Information and Privacy Commissioner

Schedule 2 - Allocated Costs

Year ended March 31, 2016

	2016				2015
	Expenses - Incurred by Others				
Program	Expenses [a]	Accommodation Costs [b]	Telephone Costs [c]	Total Expenses	Total Expenses
Operations	$ 6,917,999	$ 462,474	$ 17,155	$ 7,397,628	$ 7,322,956

[a] Expenses - Directly Incurred as per Statement of Operations.
[b] Costs shown for Accommodation (includes grants in lieu of taxes), allocated by square meters.
[c] Telephone Costs is the line charge for all phone numbers.

Appendices

Appendix A: Cases Opened under FOIP, HIA, PIPA by Entity Type 68

Appendix B: Cases Closed under FOIP, HIA, PIPA by Entity Type 71

Appendix C: Orders and Public Investigation Reports Issued 74

Appendix A: Cases Opened under FOIP, HIA, PIPA by Entity Type

Statistics are from April 1, 2015 to March 31, 2016

FOIP Entity Type	Advice and Direction	Authorization to Disregard Request	Complaint	Disclosure to Commissioner	Engage in or Commission a Study	Excuse Fees	Investigation Generated by Commissioner	Notification to OIPC	Offence Investigation	Privacy Impact Assessment	Request Authorization to Indirectly Collect	Request for Information	Request for Review	Request for Review 3rd Party	Request Time Extension	Self-reported Breach	Total
Agencies																	0
Boards			9				1						6	2			18
Colleges			1										1			1	3
Commissions			3				1			1			2			1	8
Committees												1					1
Crown Corporations																	0
Federal Departments			1														1
Foundations																	0
Government Ministries/ Departments		1	18			7	4			8		6	76	5	83	4	212
Hospital Board (Covenant Health)			1				1			1				3			6
Law Enforcement Agencies			13			1	3	6		2		1	56		5	4	91
Legislative Assembly Office																	0
Local Government Bodies			2														2
Long Term Care Centres																	0
Municipalities			14			1	1			5		1	53	16	8	8	107
Nursing Homes																	0
Office of the Premier/ Alberta Executive Council							1					1	5				7
Officers of the Legislature												1				2	3
Panels																	0
Health Quality Council of Alberta																	0
Regional Health Authorities (Alberta Health Services)		1	7			1				1			27	9		1	47
School Districts			5							2		3	19		4	12	45
Universities			3				1	1		2			7		1	4	19
Other		1	1										3			1	6
Total	**0**	**3**	**78**	**0**	**0**	**10**	**13**	**7**	**0**	**22**	**0**	**14**	**255**	**35**	**101**	**38**	**576**

Note: The statistics do not include cases

Appendix A: Cases Opened under FOIP, HIA, PIPA by Entity Type

Statistics are from April 1, 2015 to March 31, 2016

HIA

Entity Type	Advice and Direction	Authorization to Disregard Request	Complaint	Engage in or Commission a Study	Excuse Fees	Investigation Generated by Commissioner	Notification to OIPC	Offence Investigation	Privacy Impact Assessment	Request for Information	Request for Review	Request Time Extension	Self-reported Breach	Total
Affiliates and Information Managers (Electronic Medical Record Vendors, Consultants)										3			1	4
Associations, Boards, Councils, Committees, Commissions, Panels or Agencies, created by Custodians										2				2
Chiropractors									67	1			1	69
Dental Hygienists									2				1	3
Dentists													1	1
Denturists													1	1
Government Ministries/Departments														0
Health Professional Colleges and Associations										5				5
Hospital Board (Covenant Health)			2						5		1		1	9
Long Term Care Centres			1											1
Midwives														0
Minister of Health (Alberta Health)			1			1			20	6	2		44	74
Nursing Homes										1			2	3
Opticians														0
Optometrists														0
Pharmacies/Pharmacists			10			8			98		3		4	123
Physicians		1	14			6			178	3	9		19	230
Primary Care Networks									10	3			2	15
Health Quality Council of Alberta									3	1				4
Regional Health Authorities (Alberta Health Services)			43			10			15	1	11		45	125
Registered Nurses									23					23
Research Ethics Boards														0
Researchers														0
Subsidiary Health Corporations			1						4				5	10
Universities/Faculties of Medicine									2	4			1	7
Other						3		1		3			1	8
Total	**0**	**1**	**72**	**0**	**0**	**28**	**0**	**1**	**427**	**33**	**26**	**0**	**129**	**717**

Note: The statistics do not include Intake cases.

Appendix A: Cases Opened under FOIP, HIA, PIPA by Entity Type

Statistics are from the period of April 1, 2015 to March 31, 2016

PIPA Entity Type	Advice and Direction	Authorization to Disregard Request	Complaint	Engage in or Commission a Study	Excuse Fees	Investigation Generated by Commissioner	Notification to OIPC	Offence Investigation	Privacy Impact Assessment	Request for Advance Ruling	Request for Information	Request for Review	Request Time Extension	Self-reported Breach	Total
Accommodation & Food Services			4			1						2		9	16
Admin & Support Services			3			1								4	8
Arts, Entertainment & Recreation			9			1		1			1			3	15
Child Day-Care Services			1									6		5	12
Construction			7									2		2	11
Credit Bureaus			2									1			3
Credit Unions			5									1		10	16
Dealers in Automobiles			5									1		2	8
Educational Services			2								1	1		3	7
Finance			1						1					14	16
Health Care & Social Assistance			3								2	3		9	17
Information & Cultural Industries			4											9	13
Insurance Industry			5						1		1	5		12	24
Legal Services			3											3	6
Management of Companies & Enterprises			1									1			2
Manufacturing			2									1		3	6
Medical & Diagnostic Laboratories			1												1
Mining, Oil & Gas		2	9									5		10	26
Motor Vehicle Parts & Accessories			1												1
Nursing Homes/Home Health Care												5		2	7
Professional, Scientific & Technical			7			1			1			3		6	18
Public Administration														1	1
Real Estate, Rental, Leasing			25									6		4	35
Retail			1											16	17
Trades/Contractors			4									1			5
Transportation			4									1		3	8
Utilities			2								3			1	6
Wholesale Trade			2									3		2	7
Other			16			1						6		11	34
Total	0	2	129	0	0	5	0	1	3	0	8	54	0	144	~~346~~

Note: The statistics do not include intake cases.

Appendix B: Cases Closed under FOIP, HIA, PIPA by Entity Type

Statistics are from April 1, 2015 to March 31, 2016

FOIP

Entity Type	Advice and Direction	Authorization to Disregard Request	Complaint	Disclosure to Commissioner	Engage in or Commission a Study	Excuse Fees	Investigation Generated by Commissioner	Notification to OIPC	Offence Investigation	Privacy Impact Assessment	Request Authorization to Indirectly Collect	Request for Information	Request for Review	Request for Review 3rd Party	Request Time Extension	Self-reported Breach	Total
Agencies																	0
Boards		1	1										11	1			14
Colleges			2										2			1	5
Commissions						1				2			2			1	6
Committees												1	1				2
Crown Corporations													1				1
Federal Departments																	0
Foundations																	0
Government Ministries/ Departments		1	20			4	2			4		6	146	4	28	4	222
Hospital Board (Covenant Health)			1				1			1			1				4
Law Enforcement Agencies			8					4		1		1	57		3	2	76
Legislative Assembly Office																	0
Local Government Bodies			2													1	3
Long Term Care Centres																	0
Municipalities		1	19							4		1	46	9	7	10	97
Nursing Homes													1				1
Office of the Premier/ Alberta Executive Council													4	1			7
Officers of the Legislature																2	2
Panels													1				1
Health Quality Council of Alberta																	0
Regional Health Authorities (Alberta Health Services)			10										31	10		3	54
School Districts			10							4		3	21		4	16	60
Universities		1	2				1	1		1			9	1	1	4	20
Other			1										4			1	6
Total	0	4	76	0	0	6	4	7	0	18	0	12	292	31	93	48	591

Note: This statistics do not include HIA/PIPA cases.

Appendix B: Cases Closed under FOIP, HIA, PIPA by Entity Type

Statistics are from April 1, 2015 to March 31, 2016

HIA

Entity Type	Advice and Direction	Authorization to Disregard Request	Complaint	Engage in or Commission a Study	Excuse Fees	Investigation Generated by Commissioner	Notification to OIPC	Offence Investigation	Privacy Impact Assessment	Request for Information	Request for Review	Request Time Extension	Self-reported Breach	Total
Affiliates and Information Managers (Electronic Medical Record Vendors, Consultants)										4				4
Associations, Boards, Councils, Committees, Commissions, Panels or Agencies, created by Custodians										1				1
Chiropractors						1			57	1			1	60
Dental Hygienists									2					2
Dentists														0
Denturists														0
Government Ministries/Departments														0
Health Professional Colleges and Associations										3				3
Hospital Board (Covenant Health)			2			1			5		3		1	12
Long Term Care Centres														0
Midwives														0
Minister of Health (Alberta Health)			2			2			19	5	2		36	66
Nursing Homes										1	1		3	5
Opticians														0
Optometrists														0
Pharmacies/Pharmacists			5			2			95		2		4	108
Physicians		1	14		1	6			187	3	12		31	255
Primary Care Networks									6	3			1	10
Health Quality Council of Alberta									3	1				4
Regional Health Authorities (Alberta Health Services)			15			3			15	1	11		32	77
Registered Nurses									21	2				23
Research Ethics Boards														0
Researchers														0
Subsidiary Health Corporations			1						4				2	7
Universities/Faculties of Medicine						1			1	3				5
Other								1		5			1	7
Total	0	1	39	0	1	16	0	1	415	33	31	0	112	649

Note: The statistics do not include intake cases.

Appendix B: Cases Closed under FOIP, HIA, PIPA by Entity Type

Statistics are from April 1, 2015 to March 31, 2016

PIPA Entity Type	Advise and Direction	Authorization to Disregard Request	Complaint	Engage In or Commission a Study	Excuse Fees	Investigation Generated by Commissioner	Notification to OIPC	Offence Investigation	Privacy Impact Assessment	Request Advance Ruling	Request for Information	Request for Review	Request Time Extension	Self-reported Breach	Total
Accommodation & Food Services			3			1						3		3	10
Admin & Support Services			3									1		3	7
Arts, Entertainment & Recreation			1								1	1			5
Child Day-Care Services			2									9		2	13
Construction			1									2		1	4
Credit Unions			3									1		23	27
Dealers in Automobiles			6			1						1		1	9
Educational Services			2								1	1		1	5
Finance			1						1			3		9	14
Health Care & Social Assistance			1									2		5	8
Information & Cultural Industries			6								1			8	15
Insurance Industry			9			1			1		1	1		15	28
Legal Services			9									2		2	13
Management of Companies & Enterprises														1	1
Manufacturing			2									1		7	10
Mining, Oil & Gas			6									8		8	22
Motor Vehicle Parts & Accessories						1									1
Nursing Homes/Home Health Care												3		2	5
Private Health Care & Social Assistance			1									1			4
Professional, Scientific & Technical			5			1			1			3		4	14
Public Administration														1	1
Real Estate, Rental, Leasing			16									7		2	25
Retail			5			1						2		8	16
Trades/Contractors												1			1
Transportation			3									1		3	7
Utilities			1								3	1		1	8
Wholesale Trade												3		3	6
Other			19						1		1	12		12	45
Total	**0**	**0**	**111**	**0**	**0**	**6**	**0**	**0**	**4**	**0**	**8**	**70**	**0**	**125**	**324**

Note: The statistics do not include files [illegible]

Appendix C: Orders and Public Investigation Reports Issued

Statistics are from April 1, 2015 to March 31, 2016

FOIP RESPONDENT	ORDERS	PUBLIC INVESTIGATION REPORTS	TOTAL
Alberta College of Art and Design	1		1
Alberta Energy	1		1
Alberta Environment and Parks	1		1
Alberta Environment and Sustainable Resource Development		1	1
Alberta Health	1		1
Alberta Health Services	7		7
Alberta Human Rights Commission	1		1
Alberta Human Services	1		1
Alberta Jobs, Skills, Training and Labour	1		1
Alberta Justice and Solicitor General	11		11
Bow Valley College	1		1
Calgary Police Service	3		3
City of Calgary	2		2
County of St. Paul No. 19	1		1
Edmonton Police Service	2		2
Lakeshore Regional Police Service	1		1
Northwest Alberta Child and Family Services Authority (Region 8)	1		1
Office of the Premier/Executive Council	1		1
Out-of-Country Health Services Appeal Panel	1		1
Out-of-Country Health Services Committee	1		1
Peace River School Division No. 10	1		1
Service Alberta	1	1	2
University of Calgary	1		1
Sub-Total	**42**	**2**	**44**

HIA RESPONDENT	ORDERS	PUBLIC INVESTIGATION REPORTS	TOTAL
Alberta Health		1	1
Alberta Health Services	5		5
Covenant Health	1		1
Dr. Brad Mechor	1		1
Dr. Jason P. Bayne	1		1
Dr. Stephen Denson	1		1
Sub-Total	**9**	**1**	**10**

PIPA RESPONDENT	ORDERS	PUBLIC INVESTIGATION REPORTS	TOTAL
Alberta Union of Provincial Employees	1		1
College & Association of Registered Nurses of Alberta	1		1
College of Physicians and Surgeons of Alberta	1		1
Fairmont Hotels and Resorts Inc.	1		1
Gibbs Gage Architects	1		1
Grandin Manor Ltd.	1		1
Health Sciences Association of Alberta	1		1
International Brotherhood of Electrical Workers, Local Union 424	1		1
Primerica Financial Services Ltd.	1		1
Roulston Chow	1		1
St. Paul Grazing Reserve Association	1		1
Syncrude Canada Ltd.	1		1
Watch Me Grow Agency	1		1
Sub-Total	**13**	**0**	**13**
Total	**64**	**3**	**67**

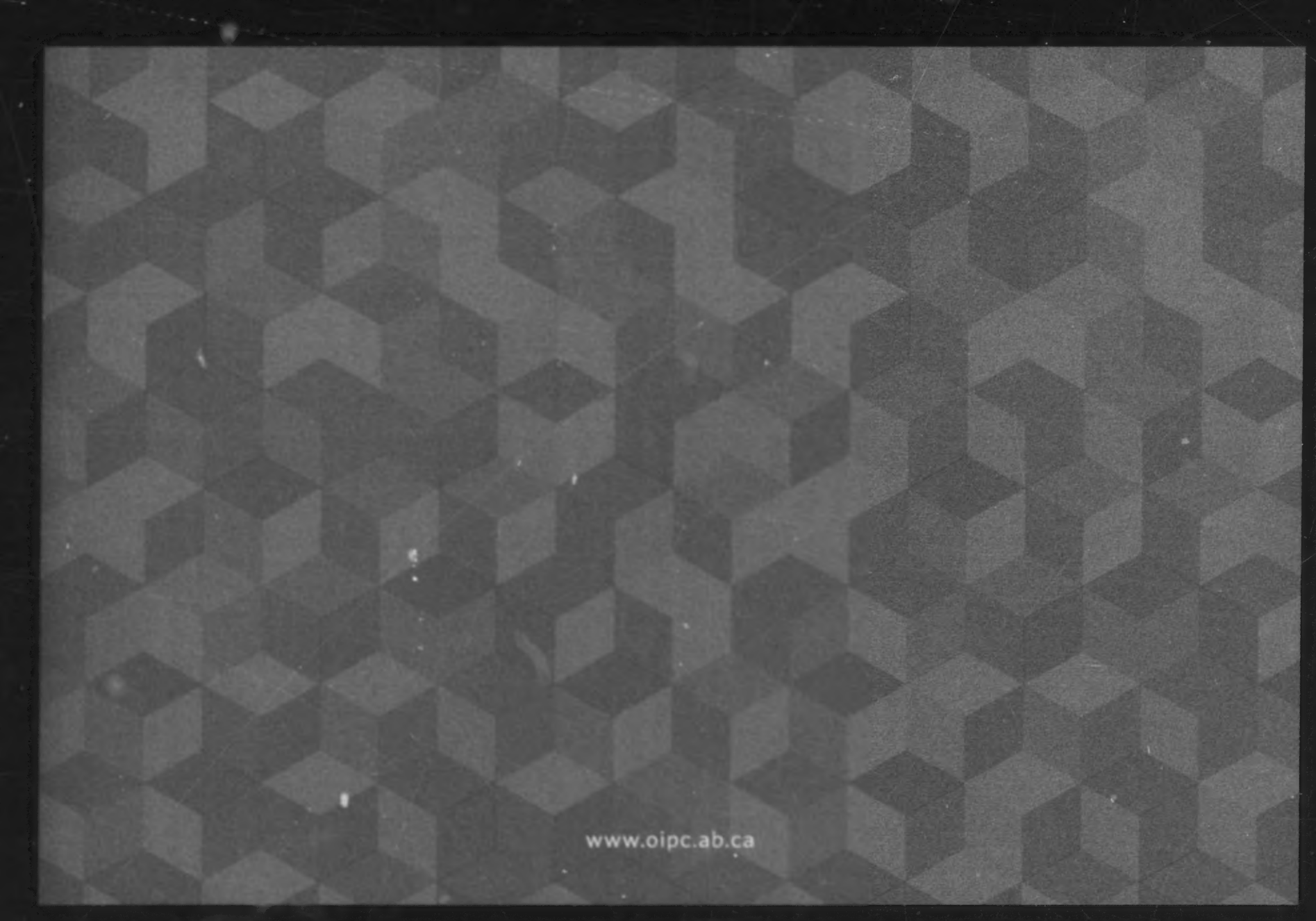
No Decisions were issued under FOIP, HIA or PIPA in 2015-16

FOIP Orders: 42 (52 cases)
FOIP Investigation Reports: 2 (3 cases)

HIA Orders: 9 (9 cases)
HIA Investigation Reports: 1 (1 case)

PIPA Orders: 13 (18 cases)
PIPA Investigation Reports: 0

Notes: A single Order or Investigation Report can relate to more than one entity and more than one file.
The number of Orders and Investigation Reports are counted by the number of Order or Investigation Report numbers assigned.
Orders are recorded by the date the Order was signed, rather than the date the Order was publicly released. Investigation Reports are recorded by the date the Investigation Report was publicly issued.
A copy of all Orders, Decisions and Public Investigation Reports are available on the OIPC web site www.oipc.ab.ca


www.oipc.ab.ca